TRAFICOM

Finnish Transport and Communications Agency
National Cyber Security Centre

Criteria to Assess the Information Security of Cloud Services (PiTuKri)

Traficom publications 20/2020
PiTuKri – version 1.1 – March 2020

Contents

Finnish Transport and Communications Agency Traficom
National Cyber Security Centre
ISBN 978-952-311-505-7

Introduction

The objective of the Criteria to Assess the Information Security of Cloud Services (PiTuKri) is to improve the security of authorities's information to be kept secret in situations where the information is processed in cloud computing environments. The criteria are intended as a tool for security assessment of cloud computing services. The criteria were prepared from the perspective of Finland's national needs. The national legislation reform initiatives have been taken into account so that the criteria also support the legislation revised at the beginning of 2020[1,2]. The preparation process made use of the BSI Cloud Computing Compliance Controls Catalogue (C5)[3], the Cloud Controls Matrix (CCM) of the Cloud Security Alliance (CSA)[4], the ISO 27001[5] and ISO 27017[6] standards as well as the Katakri criteria[7]. A further objective of the criteria is to support and make the implementation of the Ministry of Finance's Guidelines for Public Sector on Data Communications Services[8] more concrete.

The criteria address both authorities' national information to be kept secret and level IV classified information to be kept secret. The criteria also touches upon[9] the general protection principles of international RESTRICTED-level classified information. The security requirements described in the criteria are designed to keep the most typical risks facing information to be kept secret at a tolerable level. Security arrangements for information of higher classification levels are addressed only in connection with the assessment of the general applicability of cloud computing services. The criteria may also be used to protect the authorities' public information and to respond to the needs of business and industrial life.

Updated version 1.1 of the criteria specifies further the concept and use cases described in the first version[10], supplements the possibilities of application and presents other edits requested in feedback regarding, e.g., the division of requirements. The National Cyber Security Centre Finland (NCSC-FI) continues to develop the criteria. The NCSC-FI gathers feedback and further development wishes related to the criteria[11]. The feedback will be taken into account in the updated future versions of the criteria. Support tools and materials with additional information will be provided for the application of the criteria.

[1] Act on Information Management in Public Administration (906/2019). URL: https://www.finlex.fi/fi/laki/alkup/2019/20190906.

[2] Government Decree on Security Classification of Documents in Central Government (1101/2019). URL: https://www.finlex.fi/fi/laki/alkup/2019/20191101.

[3] Bundesamt für Sicherheit in der Informationstechnik. 2017. Cloud Computing Compliance Controls Catalogue (C5) - Criteria to assess the information security of cloud services. URL: https://www.bsi.bund.de/EN/C5.

[4] Cloud Security Alliance. 2018. The Cloud Security Alliance Cloud Controls Matrix (CCM). URL: https://cloudsecurityalliance.org/working-groups/cloud-controls-matrix.

[5] ISO/IEC 27001:2013 — Information technology — Security techniques — Information security management systems — Requirements.

[6] ISO/IEC 27017:2015 — Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services.

[7] Ministry of Defence of Finland. 2015. Katakri 2015 - Tietoturvallisuuden auditointityökalu viranomaisille. URL: http://www.defmin.fi/Katakri.

[8] Ministry of Finance of Finland. 2019. Julkisen hallinnon pilvipalvelulinjaukset. URL: http://urn.fi/URN:ISBN:978-952-251-982-5.

[9] International classified information is subject to originator- and owner-specific varying protection requirements that can at times differ significantly from the corresponding national requirements. Further information: ncsa (at) traficom (dot) fi.

[10] National Cyber Security Centre Finland. 2019. Criteria to Assess the Information Security of Cloud Services (PiTuKri) - v1.0.

[11] Feedback and development proposals: ncsa (at) traficom (dot) fi.

Use

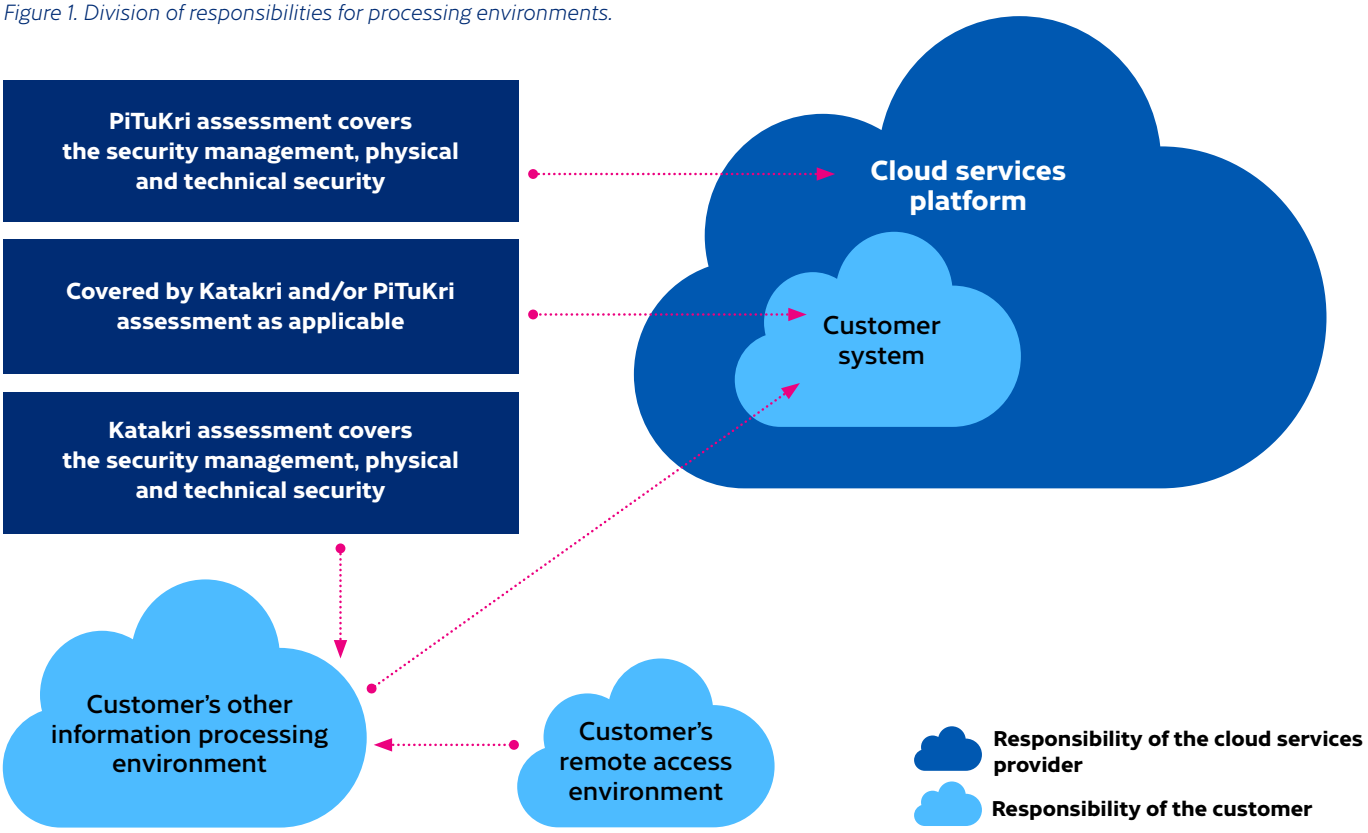
Use cases

The criteria are intended for the assessment of cloud security. They can also be used to support cloud service providers' independent information security work. The criteria have been designed to support different cloud computing services and different use cases. In order to use the criteria appropriately, their application should be use case specific.

In most use cases, the assessment of the protection of data processed in cloud services can be divided into parts for which the cloud service provider and customer are responsible[12]. The parts for which the customer is responsible typically include both the part of the customer system of the cloud service and the part of the customer's other information processing environments. The division of responsibilities for processing environments is illustrated in Figure 1. The Katakri 2015 framework can also be used in assessing the parts for which the customer is responsible.

In most use cases, it may be advisable to apply the requirements described in the criteria only to the part that the cloud service provider is responsible for; in some cases, to the parts of the service provider and the cloud service customer alike; and in some cases, only to the part that the customer is responsible for. In implementing some protections, it may be advisable to make use of the functionalities of both the customer system for which the customer is responsible and the cloud service platform for which the cloud service provider is responsible. In order to use the criteria appropriately, the security assessor, cloud service provider and cloud service customer must possess adequate competences. Examples of the allocation of the criteria to responsibilities are presented in Annex 1.

Figure 1. Division of responsibilities for processing environments.



[12] It is typically justified to include the protections of any third parties involved in the parts of the cloud service provider or customer in the assessment of the part in question. For example, in a situation in which the software development of a customer system for which the customer of the cloud service is responsible is outsourced to a third party, ensuring the security of the third party is included in the responsibilities of the customer of the cloud service.

Assessment methods

Different methods may be used for the assessment of cloud security. When assessing the protection of some types of information, it may be adequate to rely on the cloud service provider's self-assessment, possible other certifications and contractual commitments. When assessing the protection of other types of information, it is advisable to additionally require verification by an independent external party. The reliability of the verification results greatly depends on the reliability of the methods used. For instance, the degree of reliability achieved by studying documentation is not similar compared with also using technical testing for the verification of cloud service protection. It is often possible to apply, for example, continuous auditing as a source for additional evidence to improve the quality of verification. When assessing the protection of certain types of information, it is advisable to use the assessment service of the National Communications Security Authority[13]. More information about challenges related to the assessment of cloud services as well as some proposed solutions can be found in the deliverables of the EU-SEC project[14], for example.

With certain limitations, other frameworks and valid certifications may be utilised to demonstrate the fulfilment of the requirements described in the PiTuKri. When assessing the possibilities for such utilisation, it is recommended to particularly note that the different frameworks and certifications measure different things. For instance, some frameworks enable the certification of the information security management system so that the assessment of the adequacy of technical controls relies on the risk management decisions of the target organisation of the certification. This approach is different from the model generally used for the protection of classified information, in which the originator and/or owner of the information set minimum requirements for the protection of information; these requirements accompany the information throughout its life cycle in all processing environments and situations. When evaluating the possibilities for utilisation, it should also be kept in mind that certifications may be limited to cover only parts of the process or processing environment of the information to be kept secret, that the requirements of different frameworks aim for different assurance levels of protection, and that the reliability of verification of the fulfilment of the requirements also varies. Certifications against other frameworks can be utilised in the assessments; however, they do not alone enable e.g. accreditation by the National Cyber Security Centre[15].

[13] National Cyber Security Centre Finland. 2019.
URL: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/ohje_NCSA-toiminnon_suorittamat_tietoturvallisuustarkastukset.pdf.

[14] The European Security Certification Framework (EU-SEC). 2019. URL: https://www.sec-cert.eu/.

[15] The accreditation process of the National Cyber Security Centre's NCSA function is described in more detail in Annex 3.

Risk assessment

Each authority is responsible for ensuring the adequate security of its information processing. Each authority is ultimately responsible for arranging comprehensive and reliable assessment for the use case at hand and for risk-based handling of the assessment observations. In use cases where the service is offered to several central government authorities via a central service provider, it is advisable to make use of the assessments and assessment observations so that duplicate assessments are avoided. In such use cases, it should be particularly noted that the residual risks must be accepted by all of the authorities that use the service.

Appropriate use of PiTuKri requires interpreting the requirements specifically for the use case in question. Requirements may also be substituted with other protection measures of a similar level of effectiveness. The requirements or implementation examples do not describe protection measures for every environment or every special case.

It is possible to implement services on a cloud computing platform with the customer bearing significant parts of the responsibility for protection. On the other hand, particularly the availability of a service is affected by a number of factors, and a failure in any one of them may completely prevent access to the service. For instance, availability failures on the platform layer may prevent the application layer from providing the service for the customer. Similarly, even if the platform layer had been designed to support high availability, defects on the application layer may block access to the service. Access may also be prevented by a failure on the customer's device or in the connection between the device and the cloud service. On the other hand, all of the requirements described in the criteria are not as such suitable for all use cases and require case-specific assessment. It may be advisable to establish some of the protection measures on the cloud service platform and some only in the customer system. It may be advisable to establish some of the protection measures by combining the functionalities of the cloud service platform and the customer system.

The criteria can also be utilised in assessing the conformity of the protection of authorities' information to be kept secret. Annex 2 describes examples of how the criteria can be applied to the assessment of the protection of information to be kept secret and classified information to be kept secret.

In those use cases in which the goal is to achieve accreditation[15] by the competent authority for a cloud service platform or a customer system placed on the platform, the protection measures must match the risk assessment findings of both the target organisation and the competent authority. Particularly in cases involving use of compensatory controls, the target organisation must be able to demonstrate that the sufficient level of protection is achieved.

Structure

PiTuKri is divided into 11 subdivisions. Subdivision 1, Framework conditions, has a special role with respect to the other subdivisions. The framework conditions define the possibilities for further assessment and support the risk management work of the authorities responsible for the protection of information to be kept secret. For certain information to be kept secret, there are grounds for carrying out further assessment of a public, multinational cloud service, for instance. For some information, risk-based further assessment possibilities may be limited to nationally provided private cloud computing services. In the further assessment, it must be noted that the framework conditions only touch on some of the general risks. Fulfilling the framework conditions does not therefore guarantee the sufficient protection of information; the protections described in the other subdivisions must also be taken into account.

The subdivisions consist of requirement cards. A requirement card includes a description of the theme of the requirement, the concrete requirement, the scope of application, the security objective and additional information to support implementation and interpretation the requirement. The descriptions of the requirements are intended to support different ways of implementation. Some of the requirements cover the protection of information to be kept secret, while some of the requirements only address the protection of classified information. The information types addressed by the requirements are described for each requirement.

Information types

Different information types are exposed to different risks. For instance, it is generally considered that classified information of the authorities should be protected from the perspective of the security of the State (public good). On the other hand, it is reasonable to assume that actors interested in classified information are often not the same as actors interested in non-classified personal data, for instance. Information types are divided into categories based on their protection requirements. The categories are presented in Table 1.

Table 1. Types of information

Information type	Description
Public	Public information. Needs for protection are typically related to integrity and availability.
Information to be kept secret	National information of the authorities that is to be kept secret but is not classified. Most information to be kept secret of the authorities contains personal data and is, therefore, also included within the scope of personal data-related specific legislation, see information type "Personal data".
Personal data	Data pursuant to special legislation concerning the protection of personal data (including the Data Protection Act[16], Act on the Processing of Personal Data in Criminal Matters and in Connection with Maintaining National Security[17] and the EU's General Data Protection Regulation[18]).
Information to be protected from the point of view of preparedness	Information must be available also in exceptional circumstances (preparedness). In this context, 'exceptional circumstances' refer to a situation in which network connections of the society are limited to the geographical boundaries of Finland.
TL IV	Classified level IV ('KÄYTTÖ RAJOITETTU', national RESTRICTED) information of the authorities. The need for protection generally arises from the security of the State (the public interest). Protection must also take into account legislation-derived risks[19].
International RESTRICTED (KV-R)	RESTRICTED or equivalent international classified information. For example, RESTRICTED included in the scope of bilateral and multilateral agreements[20] with foreign states and international organisations. The need for protection generally arises from the security of one or more states (the public interest). Legislation-derived risks and information originator and/or owner specific special requirements must be taken into account in the protection[21].
A large quantity of information to be kept secret and/or personal data (TL IV or TL III aggregate)	Situations in which the aggregate effect is estimated to[22] result in a classified level IV ('KÄYTTÖ RAJOITETTU', national RESTRICTED) or III ('LUOTTAMUKSELLINEN', national CONFIDENTIAL) information resource. For example, some of the business secrets of companies taking part in the maintenance of Finland's critical infrastructure can be information to be kept secret alone[23], but as an aggregate covering an entity critical to the security of supply comprised of several companies, also classified[24] level III information to be kept secret.
A large quantity of TL IV information (TL III aggregate)	Situations in which the aggregate effect is estimated to result in a classified level III ('LUOTTAMUKSELLINEN', national CONFIDENTIAL) information resource. For example, a community cloud for central government in which a significant quantity of level IV information of several authorities is aggregated in such a way that the combination of the information can generate a level III information resource.
TL III and II	Level III ('LUOTTAMUKSELLINEN', national CONFIDENTIAL) and/or II ('SALAINEN', national SECRET) classified information of the authorities. The need for protection generally arises from the security of the State (the public interest). Protection must also take into account legislation-derived risks.

The division shown in Table 1 does not cover all the use cases of the authorities. For instance, preparedness involves different needs with different authorities, and the division provided addresses these only partly. It should also be taken into account in the assessment that not even a large quantity of information to be kept secret always results in the aggregate effect and the fulfilment of the grounds for[25] security classification. Appropriate use of PiTuKri requires identifying the information types being processed and assessment of the risks associated with each use case[26]. The relationship between the information types is illustrated in Figure 2.

16 Data Protection Act (1050/2018). URL: https://www.finlex.fi/fi/laki/alkup/2018/20181050

17 Act on the Processing of Personal Data in Criminal Matters and in Connection with Maintaining National Security (1054/2018). URL: https://www.finlex.fi/fi/laki/alkup/2018/20181054.

18 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj.

19 Legislation-derived risks refer to possibilities under legislation of different countries to obligate cloud service providers to cooperate with the authorities of the country in question and to provide, for instance, direct or indirect access to the cloud service customers' information to be kept secret. In addition to the physical location of information to be kept secret, legislation-derived risks may extend to disclosure of information administrated from another country through management connections. In many countries, legislation-derived disclosure and right to view data are limited to the police and the intelligence authorities.

20 Additional information about international agreements on the Ministry for Foreign Affairs website: https://um.fi/kahdenvaliset-ja-monenvaliset-sopimukset.

21 A typical special requirement is the requirement for accreditation by the national Security Accreditation Authority (SAA; in Finland the NCSA function of the Finnish Transport and Communications Agency) for all classified information processing environments.

22 The assessment requires investigating the current and expected future information content of the information aggregate in question, as well as an estimate of whether the information resource should be classified in accordance with level III, for example, under section 24, subsection 1, paragraph 2, 5 or 7–11 of the Act on the Openness of Government Activities (1999/621).

23 Typically, secrecy is based on section 24, subsection 1, paragraph 20 of the Act on the Openness of Government Activities (1999/621).

24 Secrecy and security classification may also be based on section 24, subsection 1, paragraphs 7, 8 and 10 of the Act on the Openness of Government Activities (1999/621) in some cases.

25 In accordance with the Act on Information Management in Public Administration (906/2019), a security classification marking shall be made if the document or the information included therein is secret on the basis of section 24, subsection 1, paragraphs 2, 5 or 7–11 of the Act on the Openness of Government Activities (1999/621) and the unauthorised disclosure or unauthorised use of the information contained in the document can cause prejudice to national defence, preparedness for exceptional circumstances, international relations, combating of crime, public safety or the functioning of government finances and the national economy or to the safety of Finland in another comparable manner.

26 The National Cyber Security Centre Finland supports the risk management work of the authorities through the NCSA function's assessment and accreditatio services and information security advisory service, among others. Additional information: https://www.kyberturvallisuuskeskus.fi/en/our-services/assessment-accreditation-and-guidance.

Figure 2. Types of information.

Characteristics of cloud computing services

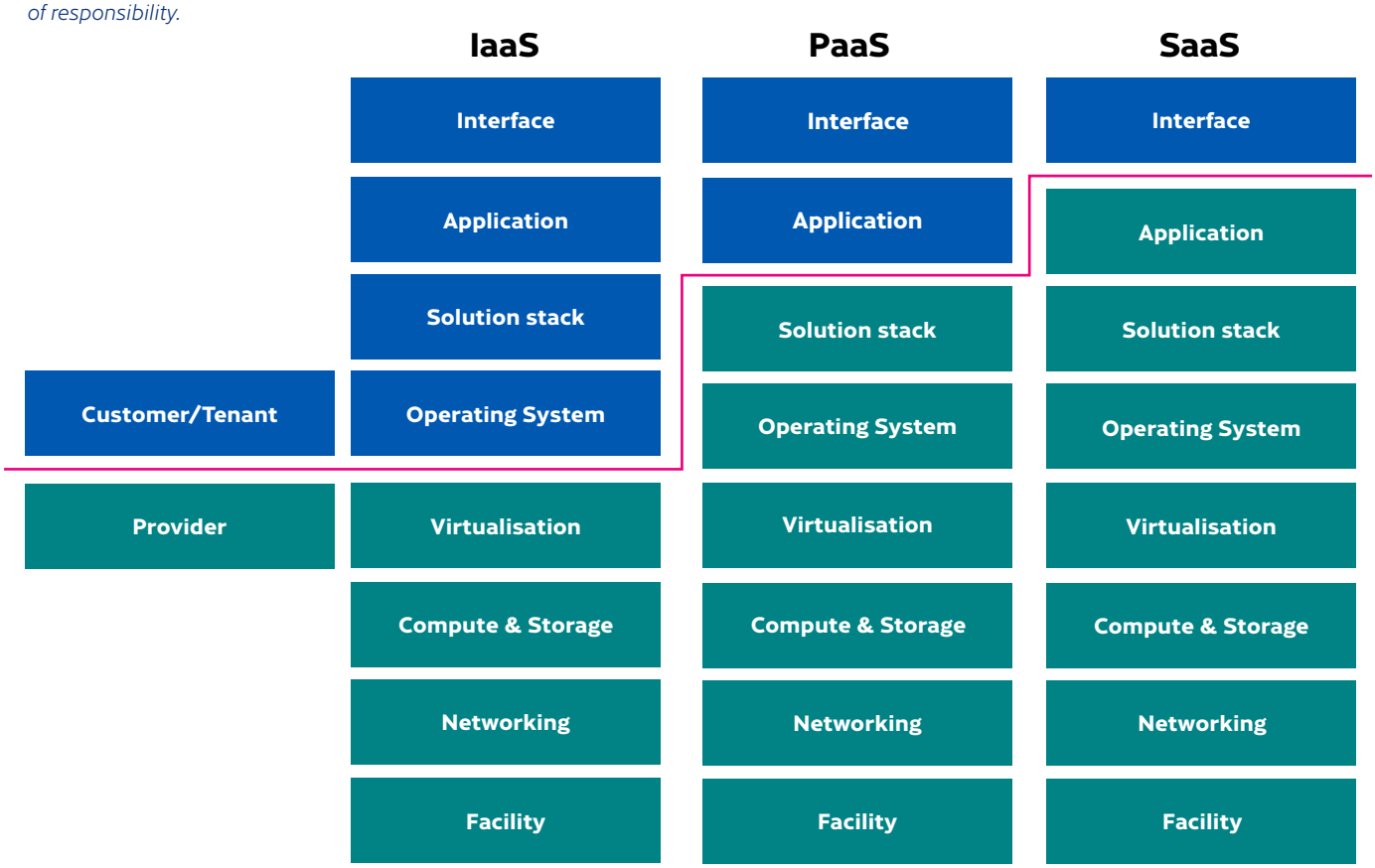
The descriptions provided in this chapter relating to cloud services are based on the definitions of NIST[27] and the concepts used in the Ministry of Finance's Guidelines for Public Sector on Data Communications. PiTuKri specifies the concepts in more detail from the security perspective, mapping them to a risk-based cloud security assessment. 'Cloud computing', or 'cloud service', refers to data processing capacity or service that is accessible over network, and which is provided applying a model of shared, scalable and flexible resources and automated to be partially provided on a self-service basis.

Cloud computing service models

The most common cloud computing service models include Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). In the IaaS model, the entire infrastructure related to providing services is acquired from the service provider. In the PaaS model, services are provided through an existing software platform. In the SaaS model, the service provider provides the services as a whole.

In each one of these models, security-related responsibilities are divided between the service provider and customer. The division of responsibilities depends on the service model and the details of the service implementation in question. The division of responsibilities associated with a PaaS service, for example, can vary even to a significant extent between different cloud service providers. A typical division of responsibilities is illustrated in Figure 3. Examples of the allocation of the criteria to responsibilities are also described in Annex 1.

Figure 3. A typical model for division of responsibility.



[27] National Institute of Standards and Technology (NIST). 2011. Special Publication 800-145: The NIST Definition of Cloud Computing. URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.

Cloud computing deployment models

The most common cloud computing deployment models are private cloud, hybrid cloud and public cloud. Other deployment models, such as community/government clouds, can usually be assessed on the basis of the most common deployment models.

Private cloud refers to service provided for exclusive use by a single organisation. The service may be operated from the service provider's and/or the user organisation's data centre. A typical strength of a private cloud is reliable isolation of the physical and logical level of the cloud service infrastructure and information processed in it[28] from other data processing environments, user organisations and external parties. Typically, a private cloud can provide services of a higher security level compared with the other deployment models.

A public cloud is a service publicly available for open use by anyone. The service is practically always provided from the service provider's data centres. In a public cloud, the cloud service infrastructure and information processed in it involve a larger attack surface than a private cloud through other users or external parties, for example.

A hybrid cloud combines a private and public cloud into a single service configuration. For instance, a private cloud on the organisation's own data centre may be supplemented with services from a public cloud. The security level achieved typically depends on the type of information that may travel from the private cloud into the public cloud and on the implementation of security measures at the interface of the cloud platforms.

[28] Usually, it is possible to limit the vulnerability surface of the cloud service infrastructure (including management and supervision solutions) used for providing private cloud service in such a way that the residual risks associated with software vulnerabilities and erroneous configurations are significantly lower than in a cloud service infrastructure also used for providing public cloud services. The internal separation of the cloud service infrastructure is discussed in more detail in requirement card JT-03.

Service provision

The cloud service provider typically has access to any unencrypted information processed through the service. Different service providers involve different risks. Service providers can be divided into the following categories:

- The organisation itself
- A national authority/public operator
- A national private operator
- A multinational authority/public operator (e.g., a community of authorities of the EU countries)
- A non-national private operator (the EU or EEA area)
- A non-national private operator (other countries)

What is essential from the security perspective is the level of assurance at which the service provider's ability and trustworthiness can be established. For instance, the trustworthiness of Finnish service providers can be assessed as part of the national Facility Security Clearance[29] process. In situations that involve more than one service provider organisation[30], risks must be assessed and taken into account for each organisation participating in the provision of service.

The following, among others, can be interpreted as national service providers:

a) A company that has been granted a national facility security clearance certificate (Act 726/2014) as follows:
   - The company's legal persons are Finnish citizens who are capable of reliably managing and being responsible for the protection of classified information with regard to administrative, physical and technological protection.
   - The company's operations are not estimated to be subject to risks materially impacting reliability, such as through the company's ownership structure. (Section 37 of Act 726/2014)
   - Persons other than Finnish citizens do not have access to system components that have material impacts on the classified information or its protections. For example, a foreign parent company/subsidiary of the company does not have access to system components that have material impact on the classified information or its protections. Borderline cases, such as a situation in which a foreign parent company/subsidiary is only granted a limited monitoring view to certain system components are subject to case-by-case assessment.
   - The classified information is physically located within the geographical borders of Finland throughout its life cycle.
     An exception is a situation in which information is protected by approved encryption when transmitted over the Internet, for example.

b) A Finnish authority. (Applying conditions similar to those above.)

[29] Additional information about the facility security clearance: https://www.supo.fi/turvallisuusselvitykset/yritysturvallisuusselvitys.

[30] An example of this is a setting in which a cloud service provider A provides a cloud computing platform on which customer B's service is implemented, with company C in charge of the maintenance and implementation of its application functionality.

Location of information and services

Location of information and services
Processing or storage of data processed by cloud computing, as well as maintenance and other administrative measures related to the provision of the cloud computing service, may reside at different geographical locations. Different locations may involve different risks associated for instance with applicable law. From the security perspective, different locations can be categorised as follows:

- Finland
- Areas enabled by data protection regulations, often the EU area/the EEA
- Other countries

Various agreements between countries or organisations may affect location-related risks. From the security perspective, also other requirements concerning the service, such as requirements related to data protection or preparedness, may set geographical limitations to the choice of cloud computing service. It is advisable to take into consideration in the assessment of location-related risks the fact that common technical encryption protections applicable to cloud services[31] do not provide significant additional protection against legislation-derived risks. It is also recommended that the EU regulation on the free flow of data (2018/1807[32]) be taken into consideration in the assessment of the possibilities, risks and requirements concerning location; however, it is not[33] applied to location requirements set on account of national security and preparedness.

[31] For example, general solution models based on the use of own keys (BYOK, Bring Your Own Keys) or Hardware Security Modules (HSM) located in the cloud service provider's physical data centre limit but do not typically prevent the cloud service provider's ability to access the data processed in the service. Cf. requirement card SA-03.

[32] Regulation (EU) 2018/1807 of the European Parliament and of the Council. 2018. URL: https://eur-lex.europa.eu/eli/reg/2018/1807/oj.

[33] Ministry of Transport and Communications report on obstacles to the mobility of non-personal data in Finland. 2019. URL: http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/161774/LVM_11_19_Muiden%20kuin%20henkil%C3%B6tietojen%20vapaan%20liikkuvuuden%20esteist%C3%A4.pdf.

Subdivision 1: Framework conditions

EE-01	System description
Requirement	1) There is a system description of the cloud computing service. The cloud service provider's description must enable the assessment of the general applicability of the service for the customer's use case in question. At least the following must be described: a) The service and deployment models and related Service Level Agreements (SLAs). b) The principles, procedures and security measures, including control measures, of the cloud computing service life cycle (development, use, disposal). c) Description of the infrastructure, network and system components used for the development, maintenance/management and use of the cloud computing service. d) Change management policies and practices, particularly the processes of changes affecting security. e) Processes for significant abnormal events, such as procedures in major system failures. f) The roles and division of responsibilities between the customer and cloud service provider relating to the provision and use of the cloud computing service. The description must clearly indicate the measures for which the customer is responsible in ensuring the security of the cloud computing service. The cloud service provider's responsibilities must include an obligation to cooperate in the resolution of incidents in particular. g) Operations transferred or outsourced to subcontractors.
Applicability	The overall security of the service provided.
Information types	Information to be kept secret, personal data, TL IV & KV-R, TL III (aggregate)
Security objective	The purpose of the description is to enable the assessment of the general applicability of the service and the assessment of risks in relation to the customer's use case.
Additional information	The description of infrastructure, network and system components must be so detailed that it can be used to evaluate the general applicability of the service and its risks in relation to the customer's use case. Cf. KT-01 (System description to promote continuity and operations security). The description of infrastructure may, to a certain extent, utilise the source code from which the infrastructure is being built. Service models include, for instance, Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). Deployment models include, for instance, private cloud, hybrid cloud and public cloud. Some cloud computing service providers offer their customer the possibility to use new functionalities that are still in the preview or testing phase. If such functionalities are considered for processing of information to be kept secret, it is recommended to consider questions such as deployment-related responsibilities in risk assessment. New functionalities may still contain security flaws, and liability for possible damage resulting from them is often assigned to the customer in agreements.

EE-02	Legislation-derived risks
Requirement	1) Any legislation-derived risks and obligations associated with the cloud computing service have been described. The descriptions prepared by the service provider must enable the assessment of the general applicability of the service for the use case in question. The descriptions must cover the entire life cycle of the use of the service and of the information processed through the service. The descriptions must include at least: a) The physical location of the information processed in the service for the entire life cycle of the information, including any subcontracting/outsourcing chains. b) The physical location of the different functions (such as maintenance/management solutions, back-ups) and components of the service for the entire life cycle of the information. c) Any other parties participating in the Service provision, such as subcontracting/outsourcing chains. d) The law applied to the use of the service and the information processed through the service as well as the place of jurisdiction. e) Parties that may, pursuant to applicable law, have access to the information processed through the service. 2) Legislation-derived risks do not limit the applicability of the cloud computing service for the use case in question. 3) The information of the cloud computing customer is kept only in the physical locations described in the agreement throughout the life cycle. An exception is a situation in which a cloud computing service customer has in advance approved in writing the transfer and processing of information in other physical locations. 4) The service provider's contractual terms and conditions do not limit the applicability of the cloud computing service for the use case in question.
Applicability	The overall security of the service provided.
Information types	Information to be kept secret, personal data, TL IV & KV-R, TL III (aggregate)
Security objective	The purpose of the description is to enable the assessment of the general applicability of the service and the assessment of risks in relation to the customer's use case.
Additional information	Legislation-derived risks refer to opportunities provided by law in different countries to obligate cloud computing service providers to cooperate with the authorities of the country in question and provide, for instance, direct or indirect access to cloud service customers' information to be kept secret. In addition to the physical location of information to be kept secret, legislation-derived risks may extend to disclosure of information from another country through management connections. In many countries, legislation-derived disclosure and right to view data are limited to the police and the intelligence authorities. 1a) and 3) In cases in which the physical location of the information may vary, the description must include all the possible locations in which information may end up during its life cycle. 4) It can be challenging for an authority to meet the obligation of section 13 of the Act on Information Management in Public Administration (906/2019) to ensure the information security of information content and information systems throughout their life cycle if the terms and conditions of agreement can be unilaterally amended. On the other hand, the processing of personal data can be prevented from the point of view of data protection regulation if the cloud service provider cannot offer an agreement compliant with the data protection regulations that cannot be amended unilaterally, i.e. without the consent of the customer of the cloud computing service. Cf. TJ-07 (Compliance and data protection). The requirements of Article 28(4) of the EU's General Data Protection Regulation and section 17, subsection 2 of the Act on the Processing of Personal Data in Criminal Matters when using "sub-processors" must be taken into consideration in the assessment. The service provider (controller) shall make a written agreement with the party processing personal data. The agreements and terms of use of cloud computing services can also involve diverse cloud service provider-specific ways of specifying the physical location countries of the service (or part thereof). The transfer of personal data outside the EU/EEA area shall always take place in accordance with the requirements laid down in the EU's General Data Protection Regulation (chapter V) or the Act on the Processing of Personal Data in Criminal Matters (chapter 7). It is recommended to apply the general principles of further assessment described in Table 2.

Table 2. Possibilities for further assessment.

Information type	Type of cloud computing service	Physical location	Service provider	Additional information
Public	No limitations	No limitations	No limitations	In the assessment of suitable protection measures, the focus is on ensuring adequate integrity and availability.
Information to be kept secret	No limitations	No limitations	No limitations	If no personal data are included. If it does include, compare with the line "Personal data" below. It should also be noted that section 13 of the Act on Information Management in Public Administration (906/2019) requires the identification of risks and scaling of protections in accordance with the risk assessment. The results of the authority's risk assessment can require more extensive protections or limitations than specified in PiTuKri.
Personal data	No limitations	Areas enabled by data protection regulations, often, e.g., Finland or/and the EU/EEA	No limitations, unless there are limitations based on a risk assessment regarding the personal data in question	The service configuration must comply with the special legislation related to the protection of personal data. The processing of personal data requires a risk assessment performed on the basis of the nature of the information, which can also result in limitations to the choice of the physical location of the information, information management and service provider.
Information to be protected from the point of view of preparedness	No limitations	Finland	A national authority/public operator/company	Information must be accessible also in exceptional circumstances (preparedness). Information management must be possible in a situation in which network connections of society are limited within the geographical boundaries of Finland. The security of a service provider can be assessed (e.g., as part of the national Facility Security Clearance process).
TL IV	No limitations	Finland	A national authority/public operator/company	Authorities of other countries must not have direct or indirect access to the information. The limitation to physical location also covers administration, back-up and other maintenance solutions. The security of a service provider can be assessed (e.g., as part of the national Facility Security Clearance process).
A large quantity of information to be kept secret and/or personal data (TL IV aggregate)	No limitations	Finland	A national authority/public operator/company	Authorities of other countries must not have direct or indirect access to the information. The limitation to physical location also covers administration, back-up and other maintenance solutions. The security of a service provider can be assessed (e.g., as part of the national Facility Security Clearance process).
International RESTRICTED (KV-R)	Private /community	Finland	A national authority/public operator/company	Authorities of other countries must not have direct or indirect access to the information. The limitation to physical location also covers administration, back-up and other maintenance solutions. The security of a service provider can be assessed (e.g., as part of the national Facility Security Clearance process). Special requirements of the classified information originator and/or owner must be taken into account in the protection. Cf. Katakri 2015.
A large quantity of information to be kept secret and/or TL IV information or/and personal data TL III (aggregate)	Private /community[34]	Finland	A national authority/public operator/company	Authorities of other countries must not have direct or indirect access to the information. The limitation to physical location also covers administration, back-up and other maintenance solutions. The security of a service provider can be assessed (e.g., as part of the national Facility Security Clearance process). With regard to the aggregate effect, such methods must be taken into account that limit access to only a single or limited part of the information content that is necessary for the task at hand and detect attempts of more extensive unauthorised access to the data content. When PiTuKri is used as the assessment tool, the aggregate effect should be interpreted so that in addition to the TL IV requirements, the protections are required to provide a security area for the physical protection of the information resource (FT-01), special reliability from the separation implementation (JT-03) and security of application layers (MH-02 / subsection 1), enhanced traceability and detection capability (JT-01 / subsections 1f-g and 4e) and reliable separation of duties (HT-05 / subsection 5). Cf. Katakri 2015 (I 01 / Additional information / Aggregate effect).
TL III ja TL II	Private/community	Finland	A national authority/public operator/company	Authorities of other countries must not have direct or indirect access to the information. The limitation to physical location also covers administration, back-up and other maintenance solutions. The security of a service provider can be assessed (e.g., as part of the national Facility Security Clearance process). Requirements for additional protection at level III and/or II must be taken into account[35], cf. Katakri 2015.

[34] A community/government cloud with certain limitations, such as a service limited to the use of government or other community of authorities.

[35] The practical implementation is usually the use of cloud technology inside physically protected security areas so that the level III/II processing environment in question is physically and logically reliably separated from other environments in their entirety.

Subdivision 2: Security management

TJ-01	Security principles
Requirement	1) The organisation has security principles approved by the senior management, describing how the organisation's security measures are linked to the organisation's activities. 2) The security principles are comprehensive and appropriate with regard to the organisation and the information being protected. 3) The security principles govern the security activities. Implementation of the security policy is reported and regularly monitored.
Applicability	The overall security of the service provided.
Information types	Information to be kept secret, personal data, TL IV & KV-R, TL III (aggregate)
Security objective	The organisation's security policy aims to ensure that the management is committed to security work in the organisation and that the security work supports the organisation's activities
Additional information	The security policy is communicated to the personnel and, where necessary, stakeholders. The policy can be presented in many ways, such as a single document or as a part of the organisation's guidelines. Valid ISO 27001 certification can support demonstrating fulfilment of the requirement, provided that the certification (including application plan) covers the processes used for the development and provision of the cloud computing service.

TJ-02	Security responsibilities
Requirement	1) The duties and responsibilities related to the management of cloud security are specified and documented. 2) The division of responsibilities between the customer and service provider relating to the provision and use of the cloud computing service are described. Cf. EE-01. 3) A person responsible for cloud service security has been appointed.
Applicability	The overall security of the service provided
Information types	Information to be kept secret, personal data, TL IV & KV-R, TL III (aggregate)
Security objective	The purpose of specifying the duties and responsibilities of security work is to ensure that persons in charge are designated to the most important domains of security and they know their responsibilities and authority.
Additional information	It is essential to specify the security responsibilities to enable the persons in charge to perform the security duties they are responsible for. If not otherwise described, all security responsibilities lie with the management of the organisation. The purpose of specifying a cloud computing policy (or a similar description) is to make clear which security duties are the responsibility of the customer and which are the responsibility of the service provider.

TJ-03	Security risk management
Requirement	1) Organisation has a risk management process in place. Risk management must be a regular, continuous and documented process. Risk management decisions and respective persons in charge are documented. 2) A systematic and comprehensible method must be used for the risk analysis. 3) Risk management must cover at least the subdivisions of security management, physical security and information assurance. 4) Identified risks related to relevant stakeholders are taken into account. The cloud service provider must ensure compliance with customer data-related obligations also in situations in which the organisation assigns data processing tasks to others. Cf. TJ-08. 5) The risk management process and its results are utilised when setting security goals for the organisation, assessing the impact of security events, planning security measures, in change management and, where applicable, in procurement. 6) Security measures are scaled taking into account the classification basis, quantity, format and storage location of the information in relation to an estimated risk of hostile or criminal activity. 7) The organisation documents the essential content of the monitoring and security measures to be applied.
Applicability	The overall security of the service provided.
Information types	Information to be kept secret, personal data, TL IV & KV-R, TL III (aggregate)
Security objective	The objective of risk management is to identify and manage factors that could potentially compromise the operation and keep any risks at a level that does not put operations and goals at risk.
Additional information	**Taking account of the legislation and regulatory requirements in security level planning** The organisation must be aware of the legislative or regulatory requirements that govern their operations. Meeting these requirements to obtain an accreditation from the authorities, for instance, may require implementing protection measures that are stricter than the organisation's internal security standards. Cf. TJ-07 (Compliance and data protection). **Allocation of risk management measures from the perspective of information to be kept secret** Risk management measures must be targeted at the environment in which the information to be kept secret is to be processed. Risk management measures may be administrative (e.g., training and instructions for the personnel) or technical (e.g., technical protection of the environment). **The principle of defence in-depth in risk management** The planning of risk management measures aims at reducing risks aimed at the operations. Defence-in-depth is a good principle to apply to the planning of these measures. This means that should an individual security arrangement fail, there are still other protection measures left. Sufficient protection against individual risks may be achieved by single reliable security measures or by combining several measures. **Risk management and analysis methods** There are many different methods available for risk management and analysis. Each one of them has its strengths and weaknesses. Many systematic methods are based on the identification of threats and vulnerabilities, assessment of probabilities and impacts, specification of risk mitigation measures, assessment of residual risk and follow-up of corrective measures.

TJ-04	Security incident management
Requirement	1) The organisation has procedures for the appropriate management of security incidents. 2) The organisation has clear processes for reporting security incidents. The organisation has designated persons/parties to whom security incidents or suspected incidents are reported. 3) The number and types of security incidents are monitored. Correction plans must aim to prevent the recurrence of incidents. 4) Security incidents and suspected security incidents relating to the processing of customer data are reported to the customer in question.
Applicability	The overall security of the service provided.
Information types	Information to be kept secret, personal data, TL IV & KV-R, TL III (aggregate)
Security objective	Security incident management aims to ensure that the organisation can function efficiently in unwanted situations, minimising damage and restoring the situation to normal. The obligation to report to the customer supports the customer's risk assessment activities and, among others, minimisation of damage.
Additional information	The following model, for instance, may be used to meet the requirement: Security incident management is 1) planned, 2) instructed and trained, 3) documented at an adequate level for the environment, 4) practiced and, in particular, 5) communication routines and responsibilities are specified. It is recommended that incidents, security breaches and attempts thereof relating to the processing of classified information in particular are reported to the National Cyber Security Centre. It is recommended to also report any detected criminal activity to the police. In addition, the short fixed period laid down in Article 33 of the EU's General Data Protection Regulation and the service provider's obligation to notify laid down in section 33 of the Act on the Processing of Personal Data in Criminal Matters must be taken into consideration.

TJ-05	Continuity management
Requirement	1) Continuity management processes and procedures are planned, implemented, tested and described in a manner that enables fulfilment of the requirements of service level agreements and law as well as other business-related requirements of the cloud computing service. The arrangements particularly take into account, that: a) adequately quick recovery and assurance of continuity with regard to the operating requirements is taken into account in the planning, b) preventive and recovery measures must be incorporated into contingency plans to minimise the effects of major failures or exceptional incidents on data processing and storage, c) observations of anomalies are included as part of risk assessment, and recovery and contingency plans are updated according to the observations and results, and d) plans related to ensuring continuity take into account the need to protect information in emergencies to prevent unauthorised access to information, disclosure of information or loss of integrity and availability.
Applicability	The overall security of the service provided.
Information types	Information to be kept secret, personal data, TL IV & KV-R, TL III (aggregate)
Security objective	The objective of continuity management is to ensure the continuity of service so that it is possible to meet the availability, integrity and confidentiality requirements associated with the service.
Additional information	The following model, for instance, may be used to meet the requirement: The effects on business are analysed and plans concerning business continuity and preparedness are verified, updated and tested at regular intervals (at least once a year) or always after substantial changes concerning the organisation or environment. The testing also concerns customers and major third parties (such as important suppliers) that are affected by these matters. The tests are documented and the results are taken into account in future security measures concerning the continuity of business. Data centre services (such as water supply, electricity, adjustment of temperature and humidity, communications and Internet connections) are ensured, monitored and maintained as well as tested at regular intervals to ensure their continuous efficiency. The services are designed to include automatic fault-resilient mechanisms and measures such as mirroring. Maintenance work is carried out in accordance with the maintenance intervals and objectives recommended by the supplier, and only authorised personnel may perform the work. Maintenance protocols and any entries in them on suspected or detected defects protocols are retained for a predefined period of time. Cf. FT-05 (Preparedness and continuity management) and KT-03 (Backup and recovery processes). In assessing the part for which the customer is responsible, it is recommended to take into account that the availability of a customer system built on a cloud computing service platform often depends directly on the functioning of the cloud computing service platform.

TJ-06	Classification and labelling of information and other assets
Requirement	1) A consistent method is in place for the classification and labelling of targets (information, equipment, software, premises) that are essential with respect to providing the cloud computing service and processing customer data. 2) Assets with information to be kept secret content (information materials, equipment and systems) are classified pursuant to legal requirements. 3) The equipment and software related to providing the cloud computing service and processing customer data are identified. 4) The equipment and software are classified according to their degree of criticality. 5) An owner/person in charge is designated for each set of equipment and software. 6) Up-to-date records are kept of equipment and software, so that any changes to the approved configuration can be detected by comparing the configuration with the records. (Cf. MH-01: Change management.)
Applicability	The overall security of the service provided.
Information types	Information to be kept secret, personal data, TL IV & KV-R, TL III (aggregate)
Security objective	The purpose of classification is the identification and correct scaling of security measures according to the need for protection. The purpose of labelling is to enable the practical implementation of the security measures according to the classification.
Additional information	Depending on the information, processing environment and users, classification may be indicated in various ways. By classifying information processing environments in accordance with the information material, it is possible to clearly indicate the security measures related to each information processing environment. To fulfil item 5 of the requirement, it is also possible to use a procedure in which the cloud service provider classifies all material produced by the customer for the service in accordance with the service provider's internal classification, so that the protection of assets (information materials, equipment and systems) with such classification meets the protection requirements for information to be kept secret and/or classified information throughout the life cycle of the information. Automated procedures are recommended for the maintenance of equipment and software records. Alternatively, the records being up-to-date can be ensured by means such as monthly manual checks. The change history of the records (the changes made) must be traceable. In assessing the part for which the customer is responsible, it is recommended to take specifically into account that a) the customer has identified the assets to be protected (customer's information materials, systems and possibly also hardware) and classified them pursuant to legal requirements, b) the customer has ensured that there are no obstacles to placing the assets to be protected in question in the cloud computing service in question (cf. EE-02), c) the customer has ensured that the cloud service provider is aware of the classification of the assets to be protected in question, and that also d) the customer has up-to-date records of the entity for which the customer is responsible so that any changes to the approved configuration can be detected by comparing the configuration with the records. (Cf. MH-01: Change management.)

TJ-07	Compliance and data protection
Requirement	1) The provisions of laws and regulations applicable to the cloud computing service and the procedures to ensure compliance have been identified, documented and regularly updated. 2) At least once a year, independent third parties carry out an audit of the operations, processes and IT systems related to the cloud computing service as applicable, in accordance with the description included in a specific audit plan. The purpose of the audit is to identify any cases that are not in compliance with the law or regulations. The assessment plan covers the security of the service in such a manner that all the most important areas affecting security are audited at least every three years. Any detected deviations are documented, prioritised and rectified according to their degree of criticality. 3) An internal audit of the functioning of the cloud computing service is performed at least once a year. The purpose of the audit is to survey how the service as a whole complies with its security practices and fulfils its contractual and legal responsibilities. The senior management is responsible for ensuring that any anomalies detected are prioritised and protection measures are replaced or rectifications made in due course.
Applicability	The overall security of the service provided.
Information types	Information to be kept secret, personal data, TL IV & KV-R, TL III (aggregate)
Security objective	Fulfilment of legal and contractual obligations.
Additional information	The cloud service provider must see to, inter alia, the security of the processing of personal data in accordance with relevant regulations; see, e.g., the Data Protection Act (1050/2018), Act on the Processing of Personal Data in Criminal Matters and in Connection with Maintaining National Security (1054/2018), and Article 32 of the General Data Protection Regulation (GDPR, (EU) 2016/679). Classification of personal data and processing according to the classification may be necessary if there are different protection needs associated with different personal data (legal requirements, value, inclusion of special categories of personal data) or/and data are processed in a different way in the cloud service provider's different functions or systems. Cf. requirement card EE-02. The authority supervising the processing of personal data in Finland is the Data Protection Ombudsman (TSV). Substantial personal data security breaches must be reported to the TSV and, if necessary, the users in accordance with Articles 33 and 34 of the GDPR. Other legislation must also be taken into account when reporting personal data breaches. For instance, Regulation (EU) No. 611/2013 regulates on telecommunications companies' obligation to report personal data security breaches to the Finnish Transport and Communications Agency and also the users, if necessary. Cf. TJ-04 (Security incident management). In assessing the part for which the customer is responsible, it is recommended to take specifically into account that the customer cannot outsource its own responsibility for compliance, including ensuring that an outsourcing partner (here, the cloud service provider in particular) meets the requirements set for the data processed.

TJ-08	Security of service providers and suppliers
Requirement	1) Customer data-related obligations are also complied with in situations in which the organisation assigns data processing tasks to others. In particular, the service provider must ensure that a) before employees of the service provider/supplier are provided with access to assets, they are subjected to the same protection measures (agreements, non-disclosure obligations, security clearance, training) as the cloud service provider, b) the service providers/suppliers have received written instructions and signed agreements under which they undertake to implement protection of at least the same level as the organisation, c) reliable procedures are in place for ensuring and controlling compliance with contractual obligations, d) service providers and suppliers who directly or indirectly participate in the processing of classified information have valid official accreditation or are included within the scope of a similar procedure. The procedure covers, as applicable, the areas of administrative (security management), physical security and information assurance.
Applicability	Security of the service provided as a whole, insofar as external service providers or/and suppliers are involved.
Information types	1a–1c: Information to be kept secret, personal data 1d: TL IV & KV-R, TL III (aggregate)
Security objective	The security of the protected targets is also ensured in circumstances in which the cloud service provider's own service providers or/and suppliers have direct or indirect access to them. Cf. MH-02 (Systems development).
Additional information	The security of the outsourcing and supply chains often has a direct effect on the protection of information processed through the cloud computing service. If the security of the cloud service provider's service to any extent relies on outsourcing or supply chains, their security must also be taken into account in the planning and maintenance of the overall security of the cloud computing service. The requirements of Article 28(4) of the EU's General Data Protection Regulation and section 17, subsection 2 of the Act on the Processing of Personal Data in Criminal Matters must also be taken into consideration when using "sub-processors". The service provider (controller) shall make a written agreement with the party processing personal data. In assessing the part for which the customer is responsible, it is recommended to take specifically into account that corresponding requirements also apply to the customer and service providers associated with the customer's part.

Subdivision 3: Personnel security

HT-01	Taking into account the different phases of employment
Requirement	1) The organisation has a procedure in place to ensure security in the different phases of employment. Particular attention is paid to measures in connection with recruitment, changes in duties, and termination of employment.
Applicability	The overall security of the service provided.
Information types	Information to be kept secret, personal data, TL IV & KV-R, TL III (aggregate)
Security objective	Mitigation of personnel-related risks during the different phases of employment.
Additional information	Security awareness typically requires instructions, which must be made available to the relevant personnel and the personnel must be trained in their application. The instructions may be divided into categories according to the phase of employment, for instance. The categories may include recruitment instructions, induction training, instructions for changes during employment, instructions for the termination of employment and instructions for more detailed measures, such as changes in access rights. In assessing the part for which the customer is responsible, it is recommended to take specifically into account that corresponding requirements also apply to the customer and any service providers associated with the customer's part.

HT-02	Assessment of personnel's trustworthiness and reliability
Requirement	1) The backgrounds of internal and external employees with access to cloud service customers' information or shared IT infrastructure are checked before the beginning of employment, using procedures enabled by local law. Within the limits allowed by law, the background check must include at least the following: a) Authentication of identity. b) Verification of job history. c) Verification of educational background. 2) The trustworthiness of individuals associated with the handling of classified information is checked and monitored by clearance procedures of a relevant level.
Applicability	The overall security of the service provided.
Information types	1: Information to be kept secret, personal data, TL IV & KV-R, TL III (aggregate) 2: TL IV & KV-R, TL III (aggregate) (employees with primary responsibility for security, technical administrators or similar employees with an access to a large quantity of TL IV information or opportunity to influence the protection of this information).
Security objective	Reduction of risks associated with personnel's' trustworthiness and reliability.
Additional information	2: If there is direct or indirect access to customers' protected information. For instance, virtualisation platform (hypervisor) administrators often in practice also have access to customer information processed in virtual machines. In assessing the part for which the customer is responsible, it is recommended to take specifically into account that corresponding requirements also apply to the customer and any service providers associated with the customer's part.

HT-03	Non-disclosure agreements and secrecy commitments
Requirement	1) A non-disclosure or secrecy commitment procedure is in place. Non-disclosure agreements must be signed before the beginning of a contractual relationship or before granting access to cloud service customers' information.
Applicability	Internal employees of the cloud service provider; employees of external service providers and suppliers.
Information types	Information to be kept secret, personal data, TL IV & KV-R, TL III (aggregate)
Security objective	Reduction of risks associated with personnel's' reliability, particularly through increased awareness.
Additional information	At least the following must be described in a non-disclosure agreement (or similar document): • Which information is subject to non-disclosure • Terms and conditions of the non-disclosure agreement • What measures should be taken at the expiry of the agreement (e.g., destroy or return the data storage media) • Who owns the information • What rules and regulations apply to the use of information to be kept secret and its disclosure to other parties, if applicable • Consequences of breaching the non-disclosure agreement In assessing the part for which the customer is responsible, it is recommended to take specifically into account that corresponding requirements also apply to the customer and any service providers associated with the customer's part.

HT-04	Security awareness
Requirement	1) The key principles and procedures relating to security are described. 2) The personnel are instructed in secure procedures so that an adequate level of security awareness can be ensured. 3) The currency and practical implementation of security-related descriptions/instructions is checked regularly and at least once a year. 4) The security-related instructions cover the processes and processing environments of personal data and information to be kept secret for the entire life cycle of the information. 5) Compliance with the security instructions is monitored and the need for changes is regularly assessed.
Applicability	Internal employees of the cloud service provider; employees of external service providers and suppliers.
Information types	Information to be kept secret, personal data, TL IV & KV-R, TL III (aggregate)
Security objective	The principles (cf. TJ 01) and descriptions/guidelines relating to security as well as their practical implementation aim to ensure that secure procedures have been planned and the personnel can also in practice act in a secure manner, including taking into account special circumstances. Cf. KT-01 (System description to promote continuity and operations security).
Additional information	It is essential to specify the security responsibilities to enable the persons in charge to perform the security duties they are responsible for. If not otherwise described, all of the security responsibilities lie with the management of the organisation. Cf. TJ-02 (Security responsibilities). The following procedure may be used to fulfil the requirement: 1) Instructions and training are provided for the personnel on appropriate handling of information to be kept secret. 2) Training on the handling of information to be kept secret is provided on a regular basis and the persons participating in the training are documented. 3) Compliance with the security instructions is monitored and need to amend the instructions is regularly assessed. 4) Information security-related security trainings and security awareness development programmes tailored for the target groups are available and mandatory for all internal and external employees of the cloud service provider. In assessing the part for which the customer is responsible, it is recommended to take specifically into account that corresponding requirements also apply to the customer and any service providers associated with the customer's part.

HT-05	Need-to-know and separation of duties
Requirement	1) A list of duties that require handling of information to be kept secret is kept. These duties also include such development and maintenance duties that enable direct or indirect access to information to be kept secret or otherwise have substantial influence on the protection of information to be kept secret. 2) Access to information to be kept secret cannot be granted, until the need-to-know related to the person's duties has been determined. 3) The list of rights to process classified information is maintained per classification level. 4) Where possible, duties and areas of responsibility are separated to reduce the risk of unauthorised or unintentional alteration or misuse of assets. If high-risk duty combinations may develop, there must be a monitoring mechanism in place to control them. 5) For a classification level III aggregate, additionally: Critical duties and areas of responsibility are separated to different persons to reduce the risk of unauthorised or unintentional alteration or misuse of assets. Particular attention must be paid to ensuring that an individual person cannot delete the traces of their actions or significantly prevent the detection of abnormal activities.
Applicability	The overall security of the service provided.
Information types	1–2: Information to be kept secret, personal data, TL IV & KV-R, TL III (aggregate) 3-4: TL IV & KV-R, TL III (aggregate) 5: TL III (aggregate)
Security objective	The security objective is to ensure that information to be kept secret can only end up with authorised persons on the need-to-know basis, in order to reduce exposure of information to be kept secret to risks.
Additional information	Determination of the need-to-know is easier when the organisation has described the principles of access to information to be kept secret by the organisation's people and a process or instructions for granting and managing task-based access in situations of change. Avoidance of high-risk job or role combinations should be taken into account in access right specifications as well as job and role specifications. In most systems, a sufficient separation of duties can be realised by separating the system maintenance roles (and persons) and roles (and persons) taking part in the monitoring of logs. Another frequently used control mechanism is that critical maintenance and other corresponding measures require the approval of two or more persons ("two person rule"). The assessment of the requirement must also consider the division of responsibilities between the cloud service provider and the customer. Typically, for instance, the cloud service provider cannot usually influence the determination of need-to-know for developers or administrators of the system section that the customer is responsible for. In assessing the part for which the customer is responsible, it is recommended to take specifically into account that corresponding requirements also apply to the customer and any service providers associated with the customer's part.

Subdivision 4: Physical security

FT-01	Defence-in-depth and risk management
Requirement	1) Physical security measures are implemented according to the principle of defence-in-depth. 2) The premises to be protected in a building are classified as physically protected security areas (administrative area, secured area), with clearly defined and visible boundaries. 3) Information resources containing at most classified level IV information to be kept secret and information systems used for processing the information must be placed in the security area. 4) Information resources forming a classified level III aggregate and information systems used for access restriction and control of the information must be placed in a secured area. 5) Administrative areas have clearly defined boundaries and only persons authorised by the organisation have access to them without an escort. 6) Secured areas have clearly specified and defined boundaries with all access in and out controlled with access permits or personal identification, and only persons whose trustworthi ness has been ensured and have a special permit to enter the area have access to them. 7) Security measures are scaled to an adequate level, so that they match the risks identified by the risk assessment.
Applicability	The overall security of the service provided.
Information types	Information to be kept secret, personal data, TL IV & KV-R, TL III (aggregate)
Security objective	The security objective is prevention of unauthorised access to the cloud service provider's data centre and information to be kept secret, as well as prevention of theft, damage, loss, financial loss and interruptions, and minimisation of their effects.
Additional information	Defence-in-depth principle means implementing a number of security measures that complement each other. If possible, areas form zones inside each other so that the innermost areas have the highest need for protection. Security measures are designed as an entity which takes into account the classification level and quantity of information to be kept secret and the environment and structure of buildings. The cloud service provider must have a risk management process in place (cf. TJ-03). The risks of premises or buildings containing sensitive or critical information, information systems or other network infrastructure are regularly assessed (at least once a year) by the cloud service provider. The risks have designated owners, persons in charge of the assessment and persons in charge of specified management measures. The risk assessment is documented. The following procedure may be used to fulfil the requirements: A building is designed so that the walls, ceiling and floor form the first protection layer. Access to the building is controlled and managed by means such as access control systems and locks. Information with a higher protection level is processed in the inner parts of the building so that intrusion into the premises would be a difficult and slow task. Security-technical solutions complement the structural solutions. The design takes into account windows, doors and other openings.

FT-02	Structures and security systems
Requirement	1) The outer limits of premises or buildings containing sensitive or critical information, information systems or other network infrastructure are protected in a physically resistant manner and with modern and appropriate security measures.
Applicability	The overall security of the service provided.
Information types	Information to be kept secret, personal data, TL IV & KV-R, TL III (aggregate).
Security objective	The security objective is prevention of unauthorised access to the cloud service provider's data centre and information to be kept secret, as well as prevention of theft, damage, loss, financial loss and interruptions, and minimisation of their effects.
Additional information	There are no special requirements for the structures of the fence defining the area or the outer walls, ceiling, floor, windows, doors and other openings of the buildings. Structures that suit the use of the buildings are adequate. The security technology must support the overall security of the area and building. Possible security measures could include a location at a sufficient distance from external parties, fences, security guards or technical surveillance systems (e.g., access control, alarm device and video surveillance systems). The systems must be regularly serviced in accordance with the manufacturer's recommendations and their working order must be ensured. Security systems and equipment must be tested (at least once a month) and kept in working order. All testing must be documented. **The following or similar procedure may be used to fulfil the requirements (TL IV):** • The structure of the walls of the building: reinforced concrete (50 mm), mineral wool for heat insulation (80 mm), reinforced concrete (60 mm). The wall structure of a data centre in which information is stored: fire board (12 mm), gypsum board + wool + gypsum board (70mm). • The entire building is protected by an access control and alarm device system. The routes leading into the data centre are provided with video surveillance. The systems are managed and monitored by an external private security company with which the organisation has signed a security contract. Responsibility for the servicing, maintenance, testing and documentation of the systems is assigned to the person in charge of security in the organisation. The functioning of the systems is tested once a month. **The following or similar procedure may be used to fulfil the requirements (TL III aggregate effect):** Data centre or building walls, floor and roof: • In terms of rigidity and construction method, the structures must be such that entry into the premises is not possible without breaking the structures with tools. • It must not be possible to remove structures or their components without damage from the outside. A class 3 burglary protection wall meets the above requirements. A partition wall structure must extend from the floor to the ceiling. • Lightweight structures must be reinforced. • The wall structures can be, for example: - 1x12 mm gypsum board + 1.5 mm steel plate + 12 mm plywood + frame + 12 mm plywood + 1.5 mm steel plate + 1x12 mm gypsum board. - Reinforced concrete; ≥ 80 mm. - Baked brick; ≥ 85 mm + 2x1.5 mm steel plate on the inside or 1.5 mm steel plate on the outside and 1.5 mm steel plate on the inside. - Walling block; ≥ 70 mm + 2x1.5 mm steel plate on the inside, alternatively 1.5 mm steel plate on the outside and 1.5 mm steel plate on the inside. Gypsum board on the steel plates. • The floor structures can be, for example: - Hollow-core slab, over 320 mm. - Concrete; ≥ 80 mm. - Other floor structures; steel plate reinforcement ≥3 mm. • The roof structures can be, for example: - Hollow-core slab. - Concrete ≥ 80 mm. - Other roof structures; steel plate reinforcement ≥3 mm. Similarly to wall and movable glass walls, glass structures must have protective glazing pursuant to standard SFS-EN 356 P6B and they must be protected with sufficiently thick security roller shutters or steel lattice.

FT-02	Structures and security systems
Additional information	**Windows and openings** The glass panes of windows must be fixed and windows closed so that they cannot be removed or opened from the outside without breaking them. Windows and skylights must be of protective glazing pursuant to SFS-EN 356 P6B or they must be protected with a fixed/locked security roller shutter, steel grid or wire net or a protection plate for openings. Other openings, such as smoke removal and air intake openings, must be secured with a fixed or locked steel grid. The protection requirement does not apply to a window or opening that is at a height of a minimum of 4 metres from the ground or other standing platform. When protecting windows and movable glass walls in other ways than with burglarproof glass, the opening size of the protective structure used must be chosen according to the size of the protected equipment so that the equipment cannot be moved through the protective structure without breaking it. **Doors, hinges and frames:** The strength of the door structure must be similar to the one of the wall structure. The door structure must be as follows: • The frame must be wedged into the structures at locks and hinges. • Security pins must be attached to frame on the hinge side at the hinges. • The gap on the lock side may not exceed 5 mm. • The operation lock of a non-rebated door must be protected with a lit plate. • The glass of the door must be fastened so that it cannot be removed from the outside without breaking it. Door glasses must be P6B burglarproof glass or protected with a roller shutter, steel grid or wire net. A door tested as class 3 according to SFS-EN 1627 meets the above requirements. **Locking:** With an operation lock with striking plates installed permanently in the door that is classified as class 1 or 2 according to SFS 7020. With a security lock with striking plates installed permanently in the door that is classified as class 3 or 4 according to SFS 7020. **Security systems:** The equipment compartment for security systems must be placed in an area corresponding to a security area. Access rights to the equipment compartment are specified based on work-based necessity. Security systems must be included in the scope of regular maintenance, updates and testing to ensure the operating condition and security of the systems. The remote connections of security systems and installation of field equipment must be carried out with sufficient security based on the risk assessment so that the security systems can only be accessed from authorised terminals/networks and the communications and security system interfaces are protected so that outsiders have no access to the transmitted data. Enhanced structural burglary protection is not, however, required if the premises are continuously staffed by security personnel. In addition, the security personnel must have sufficient supervision capability so that the police or security personnel receive an indication of intrusion so early that the intruder does not have time to gain possession of the protected information. The supervision capability can be realised through inspection rounds and real-time monitoring of the security systems or a combination of these. **Crime alarm system and alarm forwarding:** The doors, openings and windows of the protected facility must be supervised with a crime alarm system. The central units and sensors of the crime alarm system must be approved at Finance Finland category 3 as a minimum. The alarm forwarding must be realised as a supervised or duplicated connection. The alarm forwarding device must transmit at least the following information to the security company or other security control room: burglary, on/off, sabotage, fault. The system must be operated with a personal code (at least 4 digits). Only personal emergency buttons are accepted as sensors using radio. The facilities must be monitored when there is no one in them. **Access control system:** Electronic access control for entry and exit must be used at the boundary of the security area. Double identification (e.g., access code and electronic identifier) must be used for entry. Access control identifiers must use a modern and encrypted reader technology or the organisation must organise identifier management in accordance with the organisation's security guidelines (TL III + TL IV). **CCTV system:** Security areas, access routes and the surrounding area are monitored with a recording camera system. The CCTV system and recording storage period must be based on the organisation's risk assessment.

FT-03	Prevention of unauthorised access
Requirement	1) Access to rooms or buildings that include sensitive or critical information, information systems or other web infrastructure is protected and surveilled by an electronic access control system and/or mechanical/electromechanical keys to prevent unauthorised access. 2) Access management is arranged so that unauthorised access to information to be kept secret is prevented. Access to areas that include information to be kept secret is allowed only on the need-to-know basis related to work duties.
Applicability	The overall security of the service provided.
Information types	Information to be kept secret, personal data, TL IV & KV-R, TL III (aggregate).
Security objective	Only authorised persons have access to information to be kept secret processed through the cloud computing service, the equipment processing the information or the systems overseeing their security.
Additional information	The following procedure may be used to fulfil the requirements: a) The organisation uses ID cards with photographs or other similar visible identifiers that are kept visible when on premises. b) A document or log exists of the access rights granted and mechanical keys used, maintained by a designated person in charge in the organisation. The process for the granting and cancellation of access rights and mechanical keys as well as the process for lost keys is described in writing. Access rights and keys are checked regularly and according to need (at least every six months, or at the beginning and end of employment, or when a person changes job within the organisation). c) The designated person in charge of key management has a chart of the locking system and a key card. d) The access control system uses an identification system that is based on two components (e.g., identifier + PIN code). Access rights and mechanical keys are individualised for each user. If shared identifiers are used, an alternative method is in place for the reliable identification of each person. e) The mechanical keys are of a copy-protected series. The mechanical keys to the data centre are of a different series than the other keys to the building. Spare keys or an access identifier (for emergencies, etc.) are kept sealed in a locked space. The receipt of a key or access identifier can be verified afterwards. f) The keys must be stored safely and must not be marked in such a manner that they can be linked to the site. Only separate maintenance facility keys or a property route key may be stored in key deposit sunk to the external wall.

FT-04	Service providers and visitors
Requirement	1) Visitors are identified, provided with a visitor badge and recorded. The organisation has a documented visitor policy. The host principle is always applied to visitors. 2) The cleaning, maintenance and other personnel of service providers are identified, provided with a visitor badge and recorded. Regular service providers are provided with an ID card with a photograph. 3) A security clearance has been run on service providers who may independently move on premises or access protected targets. Persons on whom a security clearance cannot be run or has not yet been run always have an escort on premises. Cf. HT-02. 4) Practices related to servicing, updates and maintenance are described and documented in writing.
Applicability	The overall security of the service provided.
Information types	Information to be kept secret, personal data, TL IV & KV-R, TL III (aggregate).
Security objective	Only authorised persons assessed to be reliable have access to information to be kept secret stored the cloud computing service, the equipment processing the information or the systems overseeing their security.
Additional information	The practices and guidelines should take into account at least the following: a) ensuring the integrity of information throughout the life cycle, b) secure removal of information to be kept secret before repair or maintenance performed by an external party, c) on premises where information to be kept secret is stored and in the area outlining the premises, any maintenance work, installation and cleaning of the technical rooms and their equipment may only be carried out by security-cleared individuals who have been granted special permission to enter the secured area and who are under the supervision of the personnel of the organisation, d) agreements have been signed with the relevant service providers (e.g., fuel for spare power machines), e) the organisation has valid security agreements in place with a private security company (security services) and the company providing property maintenance services (ventilation, water, electricity, fuel, cleaning), f) response time to an alarm is such that the risk of being caught is high, g) the organisation has precautionary measures in place for maintenance and other breaks and a written description of the measures has been given to the personnel, h) any installation and maintenance work on security systems is performed by a designated company with security-cleared personnel, i) cleaning takes place once a month or as needed. The cleaners are security-cleared. The cleaners have ID cards with a photograph.

FT-05	Preparedness and continuity management
Requirement	1) Premises or buildings that contain information to be kept secret or critical information, information systems or other web infrastructure are protected from fire, water damage, explosion, unrest and other threats caused by the nature or people with structural, technical and organisational security measures. 2) At least the following security measures are implemented to protect the essential infrastructure: a) Structural security measures: Structural fire protection (fire resistance of wall, floor, ceiling and door/window structures and sealing of lead-throughs with products matching the fire resistance class). b) Technical security measures: i. The premises or building are connected to an automatic fire alarm system that alerts the emergency response centre. ii. The protected area is equipped with a ventilation system separate from the rest of the building and with automatic fire dampers (e.g., automatic smoke dampers). iii. The area is equipped with environmental condition, temperature and humidity detectors (mains current or pressure fluctuations, heat/coldness, water leaks) adequate with respect to the protected information. iv. Automatic extinguishing systems that detect a fire at an early stage and initiate first-aid extinguishing are in use. v. Undisturbed electricity supply is ensured with suitable equipment (UPS, reserve power). vi. Telecommunications backups and redundancy of the cooling system. c) Organisational security measures: i. Preparation of an emergency response plan ii. A designated person in charge or party who receives information about alarms iii. Regular emergency safety drills and fire safety inspections to verify compliance with fire safety regulations iv. Continuity planning
Applicability	The overall security of the service provided.
Information types	Information to be kept secret, personal data, TL IV & KV-R, TL III (aggregate).
Security objective	The continuity of cloud service data centres (and similar rooms) is protected against common risks.
Additional information	**Applicable security measures to promote continuity typically include the following:** **Structural protection:** - Compartmentation to confine a fire or leak - Use of fire-resistant materials (60 or 90 minutes, for example) - Fire seal products to prevent smoke and fire gases from entering other areas **Technical protection:** - Regular testing and documentation of equipment - Efficient functioning of processes and delivery of information to the right parties or individuals - Emergency cablings and connections, mirroring of systems, backup copy cycle and extent of backup copying - Failures included in contingency planning concerning full availability of a) premises b) systems c) personnel **Organisational protection:** - The purpose of the emergency response plan and continuity management is to describe the measures used to prevent, minimise, limit and recover from failures, accidents, damage and exceptional occurrences. - These plans should be updated at least annually. Critical servers and equipment must be identified and backed up in accordance with the functional requirements. Cf. TJ-05 (Continuity management) and KT-03 (Backup and recovery processes). If the functional requirements on the system are high, the availability of systems must be secured against theft, vandalism, fire, heat, gases, dust, vibration, water and failures in electricity supply. Remote access is denied to HVAC automation management monitoring critical server and equipment spaces. Environmental sensors of critical server and equipment spaces are protected and controlled. The main infrastructure of the cloud service implementation should be placed in at least two separate locations.

Subdivision 5: Communications security

TT-01	Structure of the communications network
Requirement	1) The cloud computing environment is isolated from other environments. 2) Within the perimeter, the cloud computing environment is divided into separate areas (zones, segments, microsegments or similar). 3) Traffic is monitored and controlled so that only pre-authorised traffic essential for the operation is allowed (default-deny) at the perimeter of the cloud computing environment and between the internal areas.
Applicability	Network firewalls (or similar network devices, such as routers), software firewalls on workstations and servers, other systems in the cloud computing environment (including management).
Information types	Information to be kept secret, personal data, TL IV & KV-R, TL III (aggregate).
Security objective	The purpose of limiting traffic in the service provision environment to necessary connections is to reduce the risk of attacks from unsecure networks and to limit the protected environment to a manageable size. The purpose of filtering between internal areas is to limit damage caused by possible security incidents (incl. security breaches) or attempts thereof and to improve detection of anomalies.
Additional information	Separating the data processing environment is one of the most effective factors in protecting information to be kept secret. The purpose of separation is to limit the processing environment of information to be kept secret into a managed entity, and in particular to be able to limit the processing of information to be kept secret exclusively to sufficiently safe environments. A correctly configured firewall or similar network device must be used for separation at the perimeter of the data processing environment. The firewall (or similar network device) used for the separation must also be protected against unauthorised access. The protections can also be supplemented and supported by the "Zero Trust" approach in which the possibilities of different parties to act can be limited and supervised, particularly based on the identification and authentication of actors and functions. The safe operation of connections and configurations must be ensured on a regular basis, cf. MH-01 (Change management). With regard to ensuring availability and adequate documentation, often the appropriate solution is backup copying of firewall rules and firewall configurations and adequate protection of the stored backup copies. The division of responsibilities between the service provider and customer should be considered in the interpretation of the requirement. If the purpose of assessment is to acquire a comprehensive picture of the adequacy of protection of information to be kept secret, the assessment should, as a rule, cover the sections that are the cloud service provider's responsibility as well the sections that the customer is responsible for, throughout the life cycle of the information. The assessment should consider, for example, that in the IaaS model, the cloud service provider typically cannot take a stand on the security of the configuration of software firewalls that are the customer's responsibility. On the other hand, a customer typically cannot influence the protection measures for the IaaS infrastructure platform provided by the cloud service provider. If the customer has implemented software firewalls using a software component provided by the cloud service provider, the customer typically can influence only the security of the configuration implemented by the customer on the firewalls. Therefore, in this use case, it is recommended to ensure that the cloud service provider is responsible for the software components it provides also in case of security-related deficiencies in these software components that affect the protection of the customer's information to be kept secret. In these cases, it is recommended to also consider liabilities with respect to rectification of security defects and payment of damages. In situations in which the security of the infrastructure or, for example, traffic filtering relies on software code, particular attention must be paid to software code access and version control. Cf. MH-01 (Change management), MH-02 (Systems development) and IP-03 (Management connections). On the other hand, an implementation relying of software code may, with certain limitations, enable describing the environment and assessment of its security, supported by version management. In assessing the part for which the customer is responsible, it is recommended to take specifically into account that corresponding requirements also apply to the customer's part. The requirements usually apply directly to situations in which, e.g., a customer system for which the customer is responsible has been implemented in a cloud computing service platform provided using the IaaS service model.

TT-02	Protection against common network attacks
Requirement	1) The organisation maintains a risk assessment procedure that takes into account protection against common network attacks. 2) The protection measures are scaled so that common network attacks do not compromise the confidentiality, integrity or availability of the service or the information processed through the service.
Applicability	The overall security of the service provided.
Information types	Information to be kept secret, personal data, TL IV & KV-R, TL III (aggregate).
Security objective	Access to the information processed by the cloud computing service is not prevented, or their confidentiality or integrity is not compromised as a result of common network attacks.
Additional information	All connected IT systems should basically be treated as unreliable and be prepared for common network attacks. Preparing for common network attacks also includes measures such as keeping only the necessary functionalities running. In other words, there should be a well-founded functional need for each functionality that is running. A functionality should be limited to the narrowest subset which fulfils the operational requirements (e.g., limitation of the visibility of functionalities). In addition, measures such as prevention of spoofing and limitation of the visibility of networks should be considered. Particularly at Internet interfaces, protection against (distributed) denial-of-service attacks must also be ensured. On the other hand, at some internal interfaces, the risk of denial-of-service attacks may be acceptable without specific protection measures. The interpretation of the requirement should take into account the division of responsibilities between the service provider and customer. For instance, in the IaaS model, the cloud service provider typically cannot take a stand on questions such as the fault resiliency of the customer system's software layer or the security of the configuration of software firewalls that are at the customer's responsibility. On the other hand, in the SaaS model, the cloud service provider often has considerable responsibility for the management of the denial-of-service risk, for example.

Subdivision 6: Identity and access management

IP-01	Access rights management
Requirement	1) Access rights management is based on the least privilege principle: a) A predefined process exists for the creation, approval and maintenance of user accounts. b) Users of the information processing environment are only provided with the information, rights or authorisations that are necessary for them to perform their duties. c) A list of the system users is maintained. A record is kept of each granted access right. d) When granting access rights, it is checked that the person receiving the rights is an employee or otherwise entitled. e) There are guidelines on the processing and granting of access rights. f) Access rights are kept up to date. When user accounts and rights are no longer needed (e.g., a user leaves the organisation or a user account has not been accessed for a specified period of time), they are deleted. g) A clear and efficient procedure is in place for the immediate reporting of any changes in personnel to the relevant parties as well as an efficient procedure for making the required changes. h) Access rights are regularly audited, at least every six months.
Applicability	Network devices, servers, information systems as well as workstations and other terminal devices.
Information types	Information to be kept secret, personal data, TL IV & KV-R, TL III (aggregate)..
Security objective	Access right management is based on the least privilege principle: User credentials are granted and given only to those who have a right to receive them and need them in their job/role. Access rights are limited to the necessary functionalities, applications, equipment and networks.
Additional information	It is a key aim of access rights management to be able to ensure that only authorised users have access to the data processing environment and the protected information it contains. It is recommended that there is an agreement or other documented verifiable grounds underlying the access rights (e.g., employment relationship, agreement on work to be performed in the environment). The life cycle of credentials must be managed for all user credentials so that only necessary credentials are valid and active, and unnecessary user credentials are immediately deleted. Access rights must be limited to the subdivision required by a functional need. Unnecessarily extensive rights allow the user or process in question or an attacker that gains possession of the credentials unnecessarily extensive room for action. Limiting access rights to the minimum can reduce risks from intentional and accidental actions as well as malware, for example. In particular, it should be noted that administration rights are only used for administration measures. A user account with administrator privileges should not be used for, e.g., web browsing or e-mail. Ensuring the access rights being up-to-date usually requires that the access rights of all employees, suppliers and external users are reviewed at regular intervals, such as every six months. There must be a clear and agreed procedure for modifying and deleting rights in case of changes in job description and particularly upon termination of employment. This can take place, e.g., so that the supervisor informs the persons responsible of changes in advance so that all rights can be kept up to date. This can further mean that access rights are deleted/modified from the central management system or separately from individual systems. The division of responsibilities between the cloud service provider and the customer must be considered when applying this requirement. Typically, the cloud service provider is responsible for the access rights management of the system configuration related to the provision of the cloud computing service, while the customer is responsible for the access rights management of the part that is built on the service provider's service configuration (IaaS, PaaS or SaaS). In assessing the part for which the customer is responsible, it is recommended to take specifically into account that corresponding requirements also apply to the customer and any service providers associated with the customer's part.

IP-02	User identification
Requirement	1) The service provider's and customer's administrators associated with the provision of the cloud computing service and service users are identified and authenticated reliably before access to protected information. a) Individual personal user identifiers are in use. b) All users are identified and authenticated. c) A well-known technique that is considered secure is used for the identification and authentication, or the requirement must be covered in some other reliable way. d) User identifiers are locked if authentication fails too many times in a row. e) The administration credentials for systems and applications are personal. If this is not technically possible in all systems or applications, agreed and documented management procedures enabling the identification of a user are required for identifiers in use by multiple persons. f) Authentication of users is strong, relying on at least two factors (e.g., password + token). The connection is secured with an appropriate method, preferring validated and standardised encryption solutions/protocols. Cf. SA-01. i. An exception is a situation in which authentication takes place within a physically protected security area (cf. FT-01) using at least the password. If password authentication is used, 1. users have been instructed on good practices in the choice and use of a password, 2. the application that monitors access sets up certain minimum security requirements for the password and requires changing the password at appropriate intervals. 2) In situations in which the connection passes outside the physically protected security area (e.g., between the cloud service provider's data centre and the terminal device of maintenance/customer), the data/data traffic must be protected with an encryption solution approved by the authorities. 3) The terminal devices and systems of the service provider and customer's administrators associated with the provision of the cloud computing service are identified with sufficient reliability before access to protected information.
Applicability	Network devices, servers, information systems as well as workstations and other terminal devices.
Information types	1: Information to be kept secret, personal data, TL IV & KV-R, TL III (aggregate). 2-3: TL IV & KV-R, TL III (aggregate).
Security objective	Limiting access to information and services only to authorised users.
Additional information	Setting up a reliable identification and authentication procedure includes at least the following: 1) the authentication method is protected against man-in-the-middle attacks, 2) no additional information is disclosed in the login phase, before the actual authentication of the user, 3) the authentication credentials are always in an encrypted format if they are sent across the network, 4) the authentication method is protected against replay attacks, 5) the authentication method is protected against brute force attacks. In situations in which identification in the cloud computing service uses federated identity management or/and identity and access management systems (the organisation's own or, e.g., provided by the cloud computing service provider), the assessment must pay particular attention to the trustworthiness of the Identity Provider (IdP) service and attribute chain. Only IdP services that offer strong initial identification-based identity and whose attribute chain can be realised with sufficient security up to the Relying Party (RP) or Service Provider (SP) are suited for processing information to be kept secret. Because the protection of information to be kept secret is usually directly reliant on the trustworthiness of the IdP service, ensuring the security of the IdP service is almost without exceptions part of the security assessment of a cloud computing service. For example, it is typically justified to assess the encryption protection of attribute transmission in a similar way as the transmission of the keys of the encryption solution applied to the protection of the data type in question (cf. SA-01, SA-02 and SA-03). Of the identity management models, organisation-centric identity management is usually better suited for the protection needs of information to be kept secret than, e.g., user-centric identity management; also mapping users to a specific organisation and ensuring the trustworthiness of the security implementation must also be taken into consideration. In assessing the part for which the customer is responsible, it is recommended to take specifically into account that corresponding requirements also apply to the customer and any service providers associated with the customer's part.

IP-03	Management connections
Requirement	1) In the cloud computing environment, management access takes place through limited, managed and controlled points (jump hosts, administration portals etc.). The points allowing management access are separated from each other at least so that the management points of the cloud computing service provider and different customers, and the services accessible through them, are reliably separated from each other (cf. JT-03). 2) Management access requires strong user identification based on a minimum of two authentication factors (e.g., password + token). 3) The management traffic is protected with an appropriate method, preferring validated and standardised encryption solutions/protocols. Cf. SA-01. 4) Terminal devices and other storage media (hard drives, USB memories, etc.) containing customer data taken outside of the approved physically protected security areas (cf. FT-01) are stored encrypted with an appropriate method, preferring validated and standardised encryption solutions, or the data storage media are not left unattended. Cf. SA-01 and FT-01. 5) The management of classified information of the authorities is only possible from terminal devices and environments and physical areas pursuant to the classification level in question (cf. FT-01). 6) Access to management of classified information of the authorities may only be allowed through a management connection that is encrypted with a solution approved by the authorities. 7) The encryption of terminal devices and other storage media (hard drives, USB memories etc.) containing classified information is approved by the authorities.
Applicability	Systems used for the remote management of the cloud computing environment, including network devices, servers, workstations and other terminal devices. Covers the cloud computing platform and the customer system implemented on the platform.
Information types	1-4: Information to be kept secret, personal data, TL IV & KV-R, TL III (aggregate) 5–7: TL IV & KV-R, TL III (aggregate).
Security objective	Management connections are protected at an adequate level, so that unauthorised access to customer data or the cloud service through the connections is prevented.
Additional information	In a cloud computing environment, remote management is usually the most typical management method for the actual cloud computing platform and the customer's systems alike. For instance, the cloud service provider's maintenance measures carried out from outside the physically protected data centre are considered as remote management. In addition, the cloud service customer's maintenance measures performed on a part of the system that the customer is responsible for are also considered as remote management. The assessment of the protection of management connections should particularly consider the risk of disclosure of information processed by the cloud computing service through the management connection in question. Most management connection procedures enable access to information either directly (e.g., database maintenance usually can access the content of the database when necessary) or indirectly (e.g., network device maintenance usually can change the firewall rules that protect the information system). As a rule, any means of connection that can be used to alter the protection of information to be kept secret are considered to be management connections. Typically, management connections also include web consoles/portals and other similar remote management connections provided for the cloud service customer. Especially in situations in which the management connection provides a direct or indirect access to information to be kept secret, the management connection and the terminals connected to it should be kept at the same security level as the information processing environment. Because of the security-critical nature of management traffic, the management of an environment used for the processing of classified information is not basically possible from environments or terminals with a lower level of protection. The management of a cloud computing platform that contains classified information must be limited to terminal devices that meet the security requirements for the classification level in question. It should also be noted that the terminal device management solutions and other associated backend systems must also meet the security requirements of the classification level in question, as do the physical premises/areas from which management is performed. In securing terminal devices and associated backend systems (such as directory and management services), particular attention must be paid to TT-01 (Structure of the communications network), IP-01 (Access rights management), IP-02 (User identification), IP-03 (Management connections), JT-01 (Traceability and detection capability), JT-02 (Systems hardening), JT-04 (Protection against malware), JT-05 (Transfer and removal of protected information), SA-01 (Encryption procedures and key management), SA-02 (Encryption outside a physically protected security area), KT-04 (Vulnerability management) and MH-01 (Change management) and SI-02 (Data destruction). Also the Katakri 2015 framework can be utilised in protecting the terminal devices and associated backend systems and assessing the protection. Particular attention must be paid in the management solutions of classified level III information resources, as a result of the aggregate effect, so that the terminal devices used for management shall be reliably separated from networks connected to the Internet. The so-called jump host procedure can be used to support adequate traceability; all management actions are executed and logged through the jump host. In assessing the part for which the customer is responsible, it is recommended to take specifically into account that corresponding requirements also apply to the customer and any service providers associated with the customer's part.

Subdivision 7: Information system security

JT-01	Traceability and detection capability
Requirement	1) Reliable methods are in place for tracing security events. In particular: a) Records are comprehensive enough to detect occurred or attempted security breaches afterwards. b) Essential records are kept for at least six months, unless legislation or contracts specify a longer retention period. c) Log files and respective register services are protected against unauthorised access (access rights management, logical access control) in accordance with the least privilege principle. d) The transmission of log files between the log sources and log collector is secure. The parties to the transmission are identified. Log files being transferred are encrypted with an appropriate method, preferring validated and standardised encryption solutions/protocols. Cf. SA-01. Alternatively, log files can be transmitted through a specific management network. e) Clocks are synchronised to the agreed reference time source. f) For a classification level III aggregate, additionally: Essential records are kept for at least 24 months, unless legislation or contracts specify a longer retention period. g) For a classification level III aggregate, additionally: Essential log files are sent from log sources to a separate log collector (or to separate log collectors). 2) At the customer's request and concerning the system components included within the cloud service provider's area of responsibility, the service provider provides the log files in such a format that the customer may study the cases affecting the customer. 3) The cloud service provider offers the possibility (technical interface) for real-time information exchange with the customer with regard to events associated with the safety of the customer's information (log files, event data, security findings). 4) Reliable methods are in place for the detection of security incidents. In particular: a) A procedure is in place to detect anomalies on logs (see KT-04) (in particular, an unauthorised attempt to use the information system must be detected). b) The baseline of the network traffic (volume of traffic, protocols and connections) is known. c) A procedure exists to detect abnormal events in the network traffic (e.g., abnormal connections or attempts for such). d) A procedure exists for detecting anomalies in servers and other hosts included in the cloud computing service. e) For a classification level III aggregate, additionally: A procedure exists for detecting attempts to access a more extensive part of the information content without authorisation. 5) A procedure is in place to recover from detected incidents.
Applicability	The overall security of the service provided.
Information types	1a-e, 2-3, 4a-d, 5: Information to be kept secret, personal data, TL IV & KV-R, TL III (aggregate). 1f-g, 4e: TL III (aggregate).
Security objective	Detection of any unauthorised alteration to information or other unauthorised or inappropriate information processing, including detection of security breaches and support for the planning of corrective measures.

JT-01	Traceability and detection capability
Additional information	Traceability refers to recording the events of the system environment so that, in abnormal situations, it is possible to find out what measures had been taken in the environment and by whom, and what effects such measures have had. Essential recordings typically include the log data of fundamental network devices and servers. In addition, log data of workstations, etc. are also very often covered by this. The coverage requirement can in most cases be met by checking that logging is on at least for workstations, servers, network devices (especially firewalls, but also for software firewalls on workstations). It should be possible to afterwards check from the network device logs as to what management functions were performed on the network device, when and by who. Event logs should be compiled of the use of the system, user activities as well as security-related functions and exceptions. A recommended method to protect the logs is to forward all essential logging information to a strongly safeguarded logging server (or servers), the information content of which is regularly backed up. To support the legal protection of administrators and promote investigation of suspected security breaches, it is recommended to separate tasks so that the logging data maintenance duty is separated from other maintenance duties. The functioning of logging data storage and analysis software must also be monitored. The log data storage periods must take into account the needs of the use case in question. In the activities of the authorities, for example, statutes of limitation in the criminal code can typically lead to a required storage period of at least five years. In practice, in most environments, automatic observation and alarm tools are required to be able to detect misuse attempts. Manual viewing of logging data is usually sufficient only in environments in which the logging data volume is very small and there are enough human resources to be allocated to log analysis. The restoration of an information processing environment to a protected state within reasonable time usually requires planned, described, trained and rehearsed processes and technical methods. There are many solutions available for monitoring network traffic and limiting the effects of a detected attack, ranging from monitoring at the network node level to workstation/server sensors and combinations of these. Regardless of the network devices or operators, the actual capability to detect changes at the network level typically requires understanding the baseline of the network traffic. In assessing the part for which the customer is responsible, it is recommended to take specifically into account that corresponding requirements also apply to the customer and any service providers associated with the customer's part.

JT-02	Systems hardening
Requirement	1) A procedure is used through which systems are installed systematically, resulting in a hardened configuration. 2) A hardened configuration contains only such components, services, user and process rights which are mandatory in order to fulfil the operational requirements and ensure security.
Applicability	Equipment and software related to the provision of cloud computing service. When processing classified information of the authorities, this also covers the terminal devices used for management, including their background systems (e.g., directory services).
Information types	Information to be kept secret, personal data, TL IV & KV-R, TL III (aggregate).
Security objective	. Reduces the risk of software flaws and faulty configurations by removing from use functionalities that are not needed.
Additional information	Writing secure software code has turned out to be challenging. The more software code an environment includes, the higher the risk of software flaws, that is, vulnerabilities. The higher the number of services relying on the security of software code, the more probable it is that the services also include vulnerabilities. Risks can be reduced by reducing the attack surface, that is, by exposing only the necessary services to attacks. Systems are usually full of features. These features are usually on by default and easy to take into use. On the other hand, these features are also often run with too vulnerable settings. If unnecessary features are not removed from use, they are available also for a malicious party. If the too vulnerable settings of unnecessary services are not changed, they are also available to malicious parties. By default, systems often include predefined maintenance passwords, preinstalled unnecessary software and unnecessary user accounts. Hardening of the system means, in general terms, making changes to the settings to reduce the system's attack surface. In general, only functions, equipment and services that are essential to meet the service requirements should be taken into use in systems. Similarly, for instance, automated processes should be only provided with data, rights or authorisations that are necessary to perform their tasks in order to limit damage caused by accidents, errors or unauthorised use of system resources. Configuration management tools can often also be used for security hardening and its maintenance. In assessing the part for which the customer is responsible, it is recommended to take specifically into account that corresponding requirements also apply to the customer and any service providers associated with the customer's part.

JT-03	Separation of data
Requirement	1) Customers' information to be kept secret are kept reliably separated in shared virtual or physical systems.
Applicability	Network devices, virtualisation platforms, storage systems, memory, transmission media, etc. related to the processing of customer data to be kept secret.
Information types	Information to be kept secret, personal data, TL IV & KV-R, TL III (aggregate).
Security objective	Customers' information to be kept secret can only be accessed by the customer in question.
Additional information	The separation must be adequately reliable, using either logical and/or physical separation methods. Encryption is a common separation method for shared network devices and storage systems, for instance. The customer-specific keys used for the encryption of communications (data-in-transit) and storage (data-at-rest) can also be used to support other security objectives, such as the secure disposal of equipment. Cf. SA-03 (Encryption within a physically protected security area) and KT-03 (Backup and recovery processes). If the same equipment is used for simultaneous processing of several customers' data, adequately secure physical and logical isolation of the data must be ensured. If adequate assurance of this cannot be obtained, separate physical devices must be used for the processing of data. For instance, classified information can be kept on a physically separate virtualisation platform, where potentially vulnerable processor interfaces can only be accessed by the authorised users of classified information. If the same equipment is used for the processing of several customers' data, but not simultaneously, adequately secure removal of the previous customers' data from the equipment must also be ensured (e.g., all parts, BIOS, cache memories of various other devices). If adequate assurance of this cannot be obtained, separate physical devices must be used for the processing of data. Cf. SI-02 (Data destruction). The owners of classified information may reserve themselves the right to audit all networks/systems in which their information is kept. The audit often requires physical or logical access to the environment to be audited. Therefore, it is often technically possible for the auditors to also access data processed at that environment. Especially in environments with a need to process information of multiple owners, it should be ensured that the design of the network/system enables audits without enabling owners of information to access each other's information during the audits. Particularly with the IaaS and PaaS service models, separation of classified information must be ensured physically with separate networks or encrypted virtual or software-based local networks. Cf. SA-03 (Encryption within a physically protected security area). .

JT-04	Protection against malware
Requirement	1) Reliable methods for the prevention and detection of, resilience against and recovery from malware threats are established for the cloud computing service, including the system environments used for the management of the cloud service.
Applicability	Systems used for the provision of the cloud computing service, including the system environments used for its management.
Information types	Information to be kept secret, personal data, TL IV & KV-R, TL III (aggregate)
Security objective	The integrity, confidentiality or availability of customer data are protected at an adequate level against common malware risks.
Additional information	The methods for protection against malware risks include security hardening of systems (cf. JT-02), limitation of access rights (cf. IP-01), keeping systems up-to-date with security updates (cf. KT-04), detection capability (cf. JT-01), ensuring the personnel's security awareness (cf. HT-04) and also use of anti-malware software. Risks can also be mitigated by separating high-risk environments from other production environments and, for instance, restricting the use of portable media devices, such as USB memories. In assessing the part for which the customer is responsible, it is recommended to take specifically into account that corresponding requirements also apply to the customer and any service providers associated with the customer's part. For example, if a customer system for which the customer is responsible makes it possible to load files into the customer system, malware protection is usually based on risk management.

JT-05	Transfer and removal of protected assets
Requirement	1) Equipment, software, transmission media, etc. may be transferred outside physically protected areas only with specific authorisation. 2) Transfer and processing outside physically protected areas is carried out according to the (classification of) the asset being transferred. 3) When transferring the customer's information to be kept secret outside the physically protected security area (cf. FT-01), the information is encrypted (cf. SA-02) or the protected asset is under continuous supervision of the cloud service provider's personnel. 4) In the protection of classified information of the authorities, the encryption procedures, algorithms and cryptographic products must be approved by the authorities (cf. SA-01).
Applicability	Equipment that contains customer data.
Information types	1–3: Information to be kept secret, personal data, TL IV & KV-R, TL III (aggregate)
Security objective	4: TL IV & KV-R, TL III (aggregate).
Additional information	Protected customer data are not compromised when transferred outside of physically protected areas (e.g., data centres). In particular: • Secure deletion of data and destruction of the data storage medium, cf. SI-02 (Data destruction) • Encryption of removable storage media • Transfer of data to a new data storage medium when the data storage medium is replaced In assessing the part for which the customer is responsible, it is recommended to take specifically into account that if the part for which the customer is responsible transfers information to be kept secret and/or classified information, e.g., from/to the customer's terminal devices, the information/data traffic must be encrypted with sufficient reliability.

Subdivision 8: Encryption

SA-01	Encryption procedures and key management
Requirement	1) The processes of encryption procedures and encryption key management are designed, implemented and documented. 2) Secret keys can be used by authorised users and processes only. The processes require at least a) cryptographically strong keys, b) secure key distribution, c) secure key storage, d) regular key rollovers, e) changing of outdated or disclosed keys and f) prevention of unauthorised key changes. 3) In the protection of classified information of the authorities, the encryption procedures, algorithms and cryptographic products must be approved by the authorities.
Applicability	Direct or indirect protection of customer data when the protection is carried out by encryption.
Information types	1–2: Information to be kept secret, personal data, TL IV & KV-R, TL III (aggregate) 3: TL IV & KV-R, TL III (aggregate)
Security objective	The use of encryption methods provides an adequately reliable level of protection.
Additional information	Especially when traffic passes via a public or other lower security level network, encryption solutions are often the only protections for ensuring the confidentiality, and typically also integrity, of the information to be kept secret. Because any shortcomings of encryption solutions are often extremely challenging to replace with other protections, particular attention must be paid to choice and secure usage of the encryption solution. It should also be noted that in cloud computing services in particular, the role of encryption is often also to separate different customers' information (cf. JT-03) in the jointly used infrastructure and, e.g., to support the reliability of data destruction (cf. SI-02). In protecting classified information in particular, the need for using encryption solutions with reliable evidence of their sufficient security is emphasised. Several aspects must be taken into account in the assessment of encryption solutions. In addition to verifying the strength of the algorithm and the correct functioning of the encryption solution, also the threat level of the corresponding environment must be taken into account. For instance, in traffic across the Internet, the threat level is considerably higher compared with transferring encrypted information within a managed and protected physical area (for example, traffic between two secured areas via an administrative area). Other aspects to be taken into account when assessing the encryption solution include requirements of the use case on the secrecy period and integrity of the information. Different information types are exposed to different risks. For instance, it is generally considered that classified information of the authorities should be protected from the perspective of the security of the State (public good). On the other hand, it is reasonable to assume that actors interested in classified information are often not the same as actors interested in non-classified personal data, for instance. The differences in the risks should also be taken into consideration in the choice of encryption solutions. The protection effect of encryption may be fully or partially lost in situations in which the weaknesses of key management can be exploited by unauthorised actors. The management processes of the encryption solution encryption keys must be planned, implemented and described/instructed. With regard to encryption solutions in particular, the risk assessment also needs to take into account the security of supply chains. Even if the encryption solution is sufficiently secure when leaving the provider of the encryption solutions, shortcomings in the protection of the supply chain can facilitate tampering with the encryption solution and thereby result in the deployment of an insecure encryption solution as part of the information system or service. Cf. SA-02 (Encryption outside a physically protected security area) and SA-03 (Encryption within a physically protected security area). More information is available from the National Cyber Security Centre. In assessing the part for which the customer is responsible, it is recommended to take specifically into account that corresponding requirements also apply to the customer and any service providers associated with the customer's part.

SA-02	Encryption outside a physically protected security area
Requirement	1) When transferring a customer's information to be kept secret outside approved physically protected security areas (e.g., the service provider's data centre, cf. FT-01) or through a network with a lower security level, the information to be kept secret is transferred encrypted with an appropriate method, preferring validated and standardised encryption solutions/protocols. Cf. SA-01. 2) The transfer of the information must be organised so that the recipient is verified or identified with a sufficiently secure method before the recipient gets to process the transferred information to be kept secret. 3) Classified information of the authorities is encrypted using a method approved by the authorities (cf. SA-01).
Applicability	Encryption solutions between data centres, encryption solutions for traffic through other networks with a lower security level.
Information types	1–2: Information to be kept secret, personal data, TL IV & KV-R, TL III (aggregate). 3: TL IV & KV-R, TL III (aggregate).
Security objective	The confidentiality or integrity of customer data is not compromised in transfer through unreliable networks.
Additional information	The Internet as well MPLS networks provided by operators and so-called dark fibre are considered public networks. Use of a radio interface on wireless network connections (e.g., WLAN, 4G) is interpreted as exiting a physically protected security area. In other words, use of the radio interface is considered equal to traffic through public networks, which should be taken into account particularly in the encryption of traffic. In assessing the part for which the customer is responsible, it is recommended to take specifically into account that corresponding requirements also apply to the customer and any service providers associated with the customer's part.

SA-03	Encryption within a physically protected security area
Requirement	1) When a customer's information to be kept secret is transferred within approved physically protected security areas (cf. FT-01) and within a network of the same security level, lower-level encryption or unencrypted transfer may be used, provided that adequate protection of the information can be achieved by means of physical protection. Cf. JT-03. 2) Customers' information to be kept secret is stored in the cloud computing service in an encrypted format if shared equipment is used. Cf. JT-03. 3) Encryption keys are separated on a customer-specific basis. 4) Classified information of the authorities is encrypted using a method approved by the authorities (cf. SA-01).
Applicability	Customer data processing environments in a cloud computing configuration, including file system and backup solutions.
Information types	1–3: Information to be kept secret, personal data, TL IV & KV-R, TL III (aggregate) 4: TL IV & KV-R, TL III (aggregate)
Security objective	Supporting the separation protection of different customers' information with encryption-technical methods when information of different customers is processed on shared equipment. Implementation of multilevel protection, supporting protection throughout the life cycle.
Additional information	2: Does not apply to metadata related to invoicing or other management of customer relationships. Generally, it should be kept in mind that, as a rule, the cloud service provider always has access to the information processed in the service if the information during its life cycle exists in its decrypted format (e.g., an image shown to customers). For instance, common solution models that are based on the use of own keys (BYOK, Bring Your Own Keys) or equipment-based security modules placed in the service provider's physical data centre (HSM, Hardware Security Model) limit but do not typically prevent the cloud service provider's access to the information processed by the service. However, encryption can be used for supplementary protection to support, for instance, the separation of the data of different customers, the destruction process of assets or separation of duties. Cf. JT-03 (Separation of data). Encryption is often particularly advisable for the combination of the scalability of cloud computing services and customer-specific separation. In assessing the part for which the customer is responsible, it is recommended to take specifically into account that in several cloud computing service solutions, the customer data encryption policy is partly the responsibility of the customer and configurable by the customer.

Subdivision 9: Operations security

KT-01	System description to promote continuity and operations security
Requirement	1) Comprehensive system descriptions exist of the cloud computing service as well as instructions for secure maintenance and management of the service. The descriptions and instructions are at such a level that it is possible to reliably avoid errors during use and ensure recovery from disruptions pursuant to contractual obligations. 2) The system descriptions and instructions are kept up to date. 3) The system descriptions and instructions are implemented in practice for the personnel and made available according to role.
Applicability	The cloud computing service as a whole.
Information types	Information to be kept secret, personal data, TL IV & KV-R, TL III (aggregate).
Security objective	The objective is to avoid failures during use and ensure recovery from disruptions pursuant to contractual obligations.
Additional information	In particular, if an important system component of the cloud computing service fails, adequate documentation of the system must exist to support the restoration of service. The documentation must be accessible to those individuals who need them for recovery measures. The documentation also provides support when key persons are unable to rectify an abnormal situation. Adequate documentation and instructions must also exist for situations in which the customer or a third party authorised by the customer maintains or develops a customer system on the cloud service platform. Continuity can also be supported by means such as automated correction of failures (e.g., restart of containers). In assessing the part for which the customer is responsible, it is recommended to take specifically into account that corresponding requirements also apply to the customer and any service providers associated with the customer's part.

KT-02	Capacity management
Requirement	1) The capacity of the cloud computing service is designed so that the service level pursuant to the service level agreements can be reliably provided. The design must include monitoring of the actual capacity need as well as forecast for future capacity needs. 2) The cloud service provider must facilitate monitoring the use of system resources (e.g., data processing or storage capacity) assigned to the customer.
Applicability	The cloud computing service as a whole.
Information types	Information to be kept secret, personal data, TL IV & KV-R, TL III (aggregate).
Security objective	The objective is to be able to reliably provide the service level specified in service level agreements.
Additional information	Monitoring of capacity demands helps the optimisation of resource utilisation rate, assessment of future needs as well as fulfilment of obligations pursuant to service level agreements.

KT-03	Backup and recovery processes
Requirement	1) Backup and recovery processes are designed, implemented, tested and documented as part of the contingency plan, so that the obligations pursuant to service level agreements and law as well as other business requirements of the cloud service can be fulfilled. In particular: a) Backup frequency is adequate considering the criticality of the data being backed up. Requires determining how much data may be lost (recovery point objective, RPO). b) The speed of the recovery process is adequate for the operational requirements. Requires determining how long recovery may take (recovery time objective, RTO). c) The correct functioning of backing up and the recovery process is regularly ensured through testing. d) The physical location of backup copies is adequately isolated from the actual system (separate sag/fire space, sufficient distance between backups and the system room.). 2) Backup copies are protected throughout their life cycle with methods of at least the same level as the original data. A high quantity of data may require stricter protection (aggregate effect). In particular: a) Access to backup copies is limited in accordance with the least privilege principle to approved individuals or roles. b) The backup and recovery processes are traceable (logging) and controlled so that it is possible to detect unauthorised activity (e.g., unauthorised recovery runs). c) When backup copies are kept in a different physical location, the management of physical and logical access to this location must be at least at the same level. d) When backup copies are transferred outside the physically protected security area (e.g., to another data centre of the cloud service provider) through a network, the information/communication must be encrypted with an appropriate method, preferring validated and standardised encryption solutions/protocols. Cf. SA-02 and SA-03. e) When backup copies are transferred outside the physically protected security area (cf. FT-01) on a transmission media (e.g., backup tapes or disks), the transmission media is transferred under continuous supervision. It is recommended to encrypt the transmission media or the data it contains. f) Backup media must be reliably destroyed (cf. SI-02). 3) For backup copies containing classified information of the authorities, the following must also be taken into account: a) When backup copies are transferred outside the physically protected security area (cf. FT-01) (e.g., to another data centre of the cloud service provider) through a network, the information/communication must be encrypted with an encryption solution approved by the authorities. b) When processing data of different owners in the same backup system, separation procedures (e.g., encryption and/or physically separate storage systems and media) are implemented for backup system interfaces and storage media. Cf. JT-03 and SA-03.
Applicability	Cloud service backup and recovery processes. Situations in which some processes depend on the implementation of the customer system must also be taken into account.
Information types	1–2: Information to be kept secret, personal data, TL IV & KV-R, TL III (aggregate) 3: TL IV & KV-R, TL III (aggregate)
Security objective	Protection of the availability, integrity and confidentiality of customer data in the backup and recovery processes.
Additional information	Recovery testing may also be automated to be run once a week, for example. Recovery of data must also be protected at least at the same level as the original data (including destruction, cf. SI-02). In assessing the part for which the customer is responsible, it is recommended to take specifically into account that corresponding requirements also apply to the customer and any service providers associated with the customer's part. In some cases, it may be justified due to preparedness needs, for example, that the information processed by the customer system or/and infrastructure is backed-up/duplicated also in an environment fully managed by the customer.

KT-04	Vulnerability management
Requirement	1) Reliable methods are implemented for the entire life cycle of the cloud computing service to manage software vulnerabilities. In particular: a) Security bulletins of the authorities, equipment manufacturers, software suppliers and other similar parties are followed and security updates deemed necessary based on a risk assessment are installed in a controlled manner (cf. MH-01). b) The systems are automatically checked for known vulnerabilities at least once a month. If the planned settings or the security update level are departed from, the reasons are analysed and any deviations are corrected or documented in accordance with the security incident management process (see TJ-04). c) Components essential for the secure operation of the cloud computing service are regularly (at least once a year) tested using penetration tests of an independent party. Any significant deviations from normal are immediately corrected. d) The cloud service customers are informed about any significant vulnerabilities and their effects on the protection of customer data. Communication is particularly important in situations in which vulnerability management requires measures of the cloud service provider and the customer alike.
Applicability	The software and equipment included in the cloud computing service configuration.
Information types	Information to be kept secret, personal data, TL IV & KV-R, TL III (aggregate).
Security objective	Keeping software vulnerability-related risks at a tolerable level.
Additional information	Writing secure software code has turned out to be challenging. Many types of attacks exploit software failures, or vulnerabilities, to some extent. Responsible suppliers fix vulnerabilities found in their software products. Risks can be reduced by installing patches. Vulnerability management involves continuous monitoring and development of the system environment, so that software suppliers' vulnerability patches can be installed as quickly as possible. In addition, software should be kept up-to-date with the supplier's version support. No active updates are published for outdated software versions, which means that it may be impossible to repair security vulnerabilities. The effects of vulnerability patching measures on the service must be taken into account. If performing patching causes an interruption to the customer's service, it is recommended to schedule the patching so that inconvenience to the customer is minimised or to perform the patching during a previously agreed service break. It may be advisable to test the patches first in a test environment to ensure that the patches do not cause unexpected changes in the service. Active vulnerability management can be carried out by • clearly establishing responsibilities and division of duties for vulnerability patching, • monitoring system development and the security status of any software used for the provision of service, and • agreeing on continuous monitoring procedures, e.g., by scanning one's own environment to detect known vulnerabilities. B: The check covers all systems which the system as a whole interfaces with. Scheduled vulnerability scans or configuration management databases (CMDB) or similar can be utilised for checking. The installation of security updates may also use a method in which a trusted virtual machine golden image that is on par with the security updates is maintained, and the virtual machines in use are regularly replaced with this up-to-date golden image. In this solution, particular caution must be exercised with methods aiming to ensure the integrity of the golden image. In assessing the part for which the customer is responsible, it is recommended to take specifically into account that corresponding requirements also apply to the customer and any service providers associated with the customer's part.

Subdivision 10: Transferability and compatibility

SI-01	Transferability and compatibility
Requirement	1) The application programming interfaces (API) of the cloud computing service are published so that they enable interoperability with different software components and software products. 2) The cloud computing service supports commonly used formats for software transfer (such as Open Virtualization Format, Docker, Kubernetes or similar). 3) The cloud service provider provides a technical interface or other method for transmitting the customer's information to the customer in a suitable, usable and commonly compatible format. The formats are documented at an adequate level in agreements signed with the customer. 4) Secure, well-established network protocols are used for the import and export of data as well as the administration of the service, so that the confidentiality, integrity and availability of the transferred data can be ensured. 5) Encryption solutions approved by the authorities are used for transfers of the classified information of the authorities.
Applicability	The cloud computing service as a whole.
Information types	1-4: Information to be kept secret, personal data, TL IV & KV-R, TL III (aggregate) 5: TL IV & KV-R, TL III (aggregate)
Security objective	It is possible for the customer to change the cloud service provider and use a number of cloud service providers for the implementation of the customer's service. The transfer of customer data does not compromise the confidentiality, integrity or availability of the data.
Additional information	Case-specific assessment is required on how reasonable it is to require transferability in situations in which a service implemented in the cloud computing service uses the characteristics of the cloud computing platform in question for the implementation of the service. As a rule, however, it is always reasonable to require transferability of customer data (such as the content of a customer register stored in a database) in some easily machine-processable format. In assessing the part for which the customer is responsible, it is recommended to take specifically into account the encryption of information/data traffic when information to be kept secret is exported/imported to/from the service.

SI-02	Data destruction/disposal
Requirement	1) Data destruction is arranged with sufficient reliability. 2) The destruction covers the entire life cycle of the information to be kept secret insofar as the information has resided in cloud computing service. 3) A customer's information to be kept secret is reliably destroyed particularly in the following cases: a) The customer requests destruction of their data. b) The customer's agreement expires. c) Equipment servicing, maintenance and replacement (e.g., replacement of a broken disk that contains information to be kept secret of the customer). 4) The methods used for destroying classified information prevent full and partial recovery of the data.
Applicability	Storage media and similar systems that have contained customer's information that requires protection.
Information types	1–3: Information to be kept secret, personal data, TL IV & KV-R, TL III (aggregate). 4: TL IV & KV-R, TL III (aggregate).
Security objective	The confidentiality of a customer's information to be kept secret is not compromised when storage media or similar systems used for the processing of the information are taken out of use or the customer data must be deleted from the cloud service for other reasons.
Additional information	**Reliability of destruction** The reliability of the destruction of data is significantly influenced by how different data sets have been located in the cloud service during their life cycles. For example, the reliable destruction of classified information stored in unencrypted format may require the physical destruction of the storage media in question. Reliable destruction may also require that the physical and logical location of data storage during the life cycle of the data can be found out. On the other hand, if non-classified information to be kept secret is stored in the cloud only in an encrypted format that has been assessed to be adequately reliable (cf. SA-03: Encryption within a physically protected security area), residual risks may be acceptable if the set of keys used for the encryption can be reliably destroyed. The procedure can also support the destruction of personal data after the expiry of their statutory storage period. **Destruction by shredding** Shredding of materials can be performed as follows, for instance: – maximum particle size of shredded paper is 30 mm2 (DIN 66399/P5 or DIN 32757/DIN 4), – maximum particle size of shredded magnetic hard disks is 320 mm2 (DIN 66399/H-5), – maximum particle size of shredded SSD disks and USB memories is 10 mm2 (DIN 66399/E-5), and – maximum particle size of shredded optical media is 10 mm2 (DIN 66399/O-5). With the above particle sizes, shredding waste can be disposed of as normal office waste. **Destruction by overwriting** Information may be destroyed also by overwriting the storage areas that contained a customer's information to be kept secret. Particular attention must paid to the applicability of the overwriting method used for the storage medium in question, as well as the process and the parties responsible for the process. More information on destroying electronic materials is available in the guideline by the National Cyber Security Centre (available in Finnish: www.ncsa.fi > Ohjeita > "Kiintolevyjen elinkaaren hallinta - Ylikirjoitus ja uusiokäyttö"). **Destruction using combined methods** Other methods in addition to shredding may also be used for enhanced protection to ensure that the destroyed information cannot be recovered (e.g., burning shredded material or melting hard disks). The possibility to recover documents depends also on the amount of shredded material handed over to external parties. Encryption can also considerably reduce the risks associated with information to be kept secret in the different life cycle phases of information and equipment. **Details to be taken into account when destroying electronic materials** Procedures for the reliable destruction of electronic materials in particular should cover any equipment on which information to be kept secret has been stored during its service life. Reliable destruction of information to be kept secret contained by equipment components (hard disks, memories, memory cards, etc.) must be ensured particularly when a device becomes obsolete, is sent to be serviced or is included in a recycling process. If reliable erasure (such as an overwriting procedure approved by the authorities) is not possible, a component containing information to be kept secret cannot be delivered to a third party. If reliable erasure of the memory content of a device is not possible before servicing, servicing by a third party should be carried out under supervision to ensure that information to be kept secret is not disclosed during the work. Cf. reduction of residual risks by encryption (SA-03: Encryption within a physically protected security area). In assessing the part for which the customer is responsible, it is recommended to take specifically into account that if the destruction relies on encryption in some respects, the destruction of the encryption keys must take place with adequate reliability.

Subdivision 11: Change management and system development

MH-01	Change management
Requirement	1) A change management procedure that takes security into account is in place for changes made to the cloud computing service. The change management procedure also takes compliance (cf. TJ-07) and contractual obligations into account. 2) Risks associated with changes are assessed and submitted for approval to the applicable parties. 3) All changes are tested before their introduction into the production environment. 4) Testing environments are isolated from production environments. 5) Testing is designed and implemented so that it provides a reliable picture of the effects of the change before it is installed in the production environment.
Applicability	The cloud computing service as a whole.
Information types	Information to be kept secret, personal data, TL IV & KV-R, TL III (aggregate)
Security objective	The confidentiality, integrity or availability of information processed through the cloud computing service are not compromised as a result of changes made to the service.
Additional information	The following procedure may support the fulfilment of the requirements: 1) Processes are specified for rolling back of changes in case of failures or security problems and the restoration of the affected systems or services to the state preceding the changes. 2) Before introducing a change into the production environment, the success of the planned tests is evaluated and the granting of required approvals is checked. 3) In emergencies (such as a major equipment failure or security breach), a lighter change management process can be used, provided that the security effects of the changes are analysed afterwards to the same extent as in the normal process (typically, within a week of the changes at the latest). 4) The isolation of the testing environment from the production environment is reliably implemented with either physical or logical isolation methods to avoid unauthorised access and changes to the production environment and data. To protect the confidentiality of data, production data are not transferred into development or testing environments. 5) Change management procedures involve role-based rights to ensure appropriate separation of duties in the development and deployment of changes as well as the transfer of changes between environments. In assessing the part for which the customer is responsible, it is recommended to take specifically into account that corresponding requirements also apply to the customer and any service providers associated with the customer's part.

MH-02	Systems development
Requirement	1) Applications and application programming interfaces (APIs) are designed, developed, tested and deployed in accordance with good security practices of the industry. The interfaces must withstand common attack methods without compromising the confidentiality, integrity or availability of the data processed. 2) The production environment is isolated from the other environments (e.g., development, testing and quality assurance environments). 3) The security of version management is taken into account at least so that the procedures reliably prevent the transfer of unauthorised versions into the production environment. 4) The practices of secure software development process are implemented in each part of the organisation that has anything to do with the software in question. 5) In situations in which the design, development, testing or provisioning of the source code of the cloud computing service (or part thereof) is outsourced, agreements particularly take into account the following: a) The requirements of a secure software development process (particularly with respect to design, development and testing), b) evidence of adequate testing, c) acceptance testing according to the agreed operational and non-operational requirements, and d) the right to test the development process and control measures, also as spot checks.
Applicability	System development related to the cloud computing service configuration.
Information types	Information to be kept secret, personal data, TL IV & KV-R, TL III (aggregate).
Security objective	The confidentiality, integrity or availability of information processed through the cloud computing service is not compromised as a result of system development performed on the service.
Additional information	1: Security procedures include, for example, OWASP for web applications and system development life cycle models (SDLC, Systems Development Life Cycle). 5: Cf. TJ-08 (Security of service providers and suppliers). In assessing the part for which the customer is responsible, it is recommended to take specifically into account that corresponding requirements also apply to the customer and any service providers associated with the customer's part.

Annex 1: Examples of application of the requirements

This Annex describes examples of the allocation of the requirements described in PiTuKri. The examples are divided into the customer's and cloud service provider's responsibilities by service model. The imaginary cloud computing service used in the examples is realised using a common responsibility matrix, presented in Figure 3.

Note: The practical instances of cloud computing services differ from one another with regard to both technical implementation and division of responsibilities. For example, the protection responsibilities a cloud service platform provided with the PaaS service model and a customer system implemented on top of it can differ even significantly between different service providers. A meaningful assessment thereby requires taking into account the technical implementation and division of responsibilities for the cloud service provider and customer system in question.

IaaS as the service model

This example describes the allocation of the requirements described in PiTuKri on a responsibility-specific basis when the customer system is located on a platform provided by the cloud service provider with the IaaS service model.

ID	Subitem	Responsibility/ Customer environment part	Responsibility/ Cloud service provider part
EE-01	1 a-g	-	x
EE-02	1	-	x
	2	x (assessment of applicability)	x
	3	-	x
	4	x (assessment of applicability)	x
TJ-01	1-3	x	x
TJ-02	1-3	x	x
TJ-03	1-7	x	x
TJ-04	1-3	x	x
	4	-	x
TJ-05	1 a-d	x (where applicable)	x
TJ-06	1-6	x	x
TJ-07	1-4	x	x
TJ-08	1 a-d	x	x
HT-01	1	x	x
HT-02	1-2	x	x
HT-03	1	x	x
HT-04	1-5	x	x
HT-05	1-4	x	x
FT-01	1-4	-	x
FT-02	1	-	x
FT-03	1-2	-	x
FT-04	1-4	-	x
FT-05	1-2	-	x
TT-01	1-3	x	x
TT-02	1-2	x	x
IP-01	1 a-h	x	x
IP-02	1-3	x	x
IP-03	1	-	x
	2-7	x	x
JT-01	1	x	x
	2-3	-	x
	4-5	x	x
JT-02	1-2	x	x
JT-03	1	- (Unless the customer system has customer data)	x
JT-04	1	x	x

ID	Subitem	Responsibility/ Customer environment part	Responsibility/ Cloud service provider part
JT-05	1-4	-	x
SA-01	1-3	x	x
SA-02	1-3	x	x
SA-03	1	-	x
	2-4	x	x
KT-01	1-3	x	x
KT-02	1	-	x
	2	-	x
KT-03	1	x	x
	2 a-c	x	x
	2 d	x (if the customer carries out the transfer through/using the customer environment)	x
	2 e-f	-	x
	3	x	x
KT-04	1 a-b	x	x
	1 c-d	-	x
SI-01	1-2	-	x
	3	x (with regard to the agreement)	x
	4-5	x (can apply with regard to the customer's configuration options)	x
SI-02	1-2	x	x
	3	-	x
	4	x	x
MH-01	1-5	x	x
MH-02	1-5	x	x

PaaS as the service model

This example describes the allocation of the requirements described in PiTuKri on a responsibility-specific basis when the customer system is located on a platform provided by the cloud service provider with the PaaS service model.

ID	Subitem	Responsibility/ Customer environment part	Responsibility/ Cloud service provider part
EE-01	1 a-g	-	x
EE-02	1	-	x
	2	x (assessment of applicability)	x
	3	-	x
	4	x (assessment of applicability)	x
TJ-01	1-3	x	x
TJ-02	1-3	x	x
TJ-03	1-7	x	x
TJ-04	1-3	x	x
	4	-	x
TJ-05	1 a-d	x (where applicable)	x
TJ-06	1-6	x	x
TJ-07	1-4	x	x
TJ-08	1 a-d	x	x
HT-01	1	x	x
HT-02	1-2	x	x
HT-03	1	x	x
HT-04	1-5	x	x
HT-05	1-4	x	x
FT-01	1-4	-	x
FT-02	1	-	x
FT-03	1-2	-	x
FT-04	1-4	-	x
FT-05	1-2	-	x
TT-01	1-3	x	x
TT-02	1-2	x	x
IP-01	1 a-h	x	x
IP-02	1-3	x	x
IP-03	1	-	x
	2-7	x	x
JT-01	1	x	x
	2-3	-	x
	4-5	x	x
JT-02	1-2	- (Note: Service provider-specific variation in limits of responsibility, e.g., with regard to applications.)	x
JT-03	1	- (Unless the customer system has customer data with additional separation needs.)	x

ID	Subitem	Responsibility/ Customer environment part	Responsibility/ Cloud service provider part
JT-04	1	- (Note: Service provider-specific variation in limits of responsibility.)	x
JT-05	1-4	-	x
SA-01	1-3	x	x
SA-02	1-3	x	x
SA-03	1	-	x
	2-4	x	x
KT-01	1-3	x	x
KT-02	1	-	x
	2	-	x
KT-03	1	x	x
	2 a-c	x	x
	2 d-f	-	x
	3	x	x
KT-04	1 a-b	x (Note: Service provider-specific variation in limits of responsibility, e.g., firewall software of any part for which the customer is responsible and any IAM systems for which the customer is responsible.)	x
	1 c-d	-	x
SI-01	1-2	-	x
	3	x (with regard to the agreement)	x
	4-5	x (can apply with regard to the customer's configuration options)	x
SI-02	1-2	x	x
	3	-	x
	4	x	x
MH-01	1-5	x	x
MH-02	1-5	x (Note: Service provider-specific variation.)	x

SaaS as the service model

This example describes the allocation of the requirements described in PiTuKri on a responsibility-specific basis when the customer uses the cloud service provider's application provided with the SaaS service model.

ID	Subitem	Responsibility/ Customer environment part	Responsibility/ Cloud service provider part
EE-01	1 a-g	-	x
EE-02	1	-	x
	2	x (assessment of applicability)	x
	3	-	x
	4	x (assessment of applicability)	x
TJ-01	1-3	x	x
TJ-02	1-3	x	x
TJ-03	1-7	x	x
TJ-04	1-3	x	x
	4	-	x
TJ-05	1 a-d	x (Where applicable, e.g., action when network connection to the cloud computing service is not available)	x
TJ-06	1	-	x
	2	x	x
	3-4	-	x
	5	x (owner/party responsible for the parts of the applications used for which the customer is responsible)	x
	6	x (accounting and change management of the parts of the applications used and their parts for which the customer is responsible)	x
TJ-07	1-4	x (assessment of the compliance and data protection of the use of applications)	x
TJ-08	1 a-d	x	x
HT-01	1	x	x
HT-02	1-2	x	x
HT-03	1	x	x
HT-04	1-5	x	x
HT-05	1-4	x	x
FT-01	1-4	-	x
FT-02	1	-	x
FT-03	1-2	-	x
FT-04	1-4	-	x
FT-05	1-2	-	x
TT-01	1-3	-	x
TT-02	1-2	-	x
IP-01	1 a-h	x	x

ID	Subitem	Responsibility/ Customer environment part	Responsibility/ Cloud service provider part
IP-02	1-3	x (usually focusing on configuring secure settings in the settings of the service in question and on the security of the customer's terminal devices)	x
IP-03	1	-	x
	2-7	x (usually focusing on configuring secure settings in the settings of the service in question and on the security of the customer's terminal devices)	x
JT-01	1-5	-	x
JT-02	1-2	-	x
JT-03	1	-	x
JT-04	1	-	x
JT-05	1-4	-	x
SA-01	1-3	x (can apply with regard to the customer's configuration options)	x
SA-02	1-3	x (can apply with regard to the customer's configuration options)	x
SA-03	1	-	x
	2-4	x (can apply with regard to the customer's configuration options)	x
KT-01	1-2	-	x
	3	x	x
KT-02	1	-	x
	2	-	x
KT-03	1-3	-	x
KT-04	1 a-d	-	x
SI-01	1-2	-	x
	3	x (with regard to the agreement)	x
	4-5	x (can apply with regard to the customer's configuration options)	x
SI-02	1-4	- (can apply with regard to the customer's configuration options)	x
MH-01	1-2	x (emphasis usually on administrative procedures)	x
	3-5	- (can apply in custom applications in which it may be necessary for also the customer to take part in testing)	x
MH-02	1-5	-	x

Annex 2: Examples of application of the criteria to the assessment of compliance

Example 1: Assessment of the compliance of the protections of information to be kept secret

This section describes an example of how the criteria can be applied to the assessment of the compliance of the protection of non-classified information to be kept secret in terms of the requirements of the Act on Information Management in Public Administration (906/2019). The customer in the example is authority A which wants to assess the adequacy of the protections of its new information system for processing non-classified information to be kept secret. The new system is still in the design phase and is to be located on a cloud computing service.

Authority A has identified the following connections between the requirements of the Act on Information Management in Public Administration and PiTuKri concerning A's system environment:

- section 12: Identification of tasks requiring reliability and ensuring reliability: HT-02 (Assessment of personnel's trustworthiness and reliability); HT-03 (Non-disclosure agreements and secrecy commitments)
- section 14: Transfer of data in a data network: SA-02 (Encryption outside a physically protected security area) / subsections 1–2; SA-01 / subsections 1–2.
- section 16: Management of access rights to information systems: IP-01 (Access rights management)
- section 17: Log data collection: JT-01 (Traceability and detection capability) / subsections 1–3
- section 21: Determining the necessity for storage of data (destruction after the expiry of the storage period): SI-02 (Data destruction)

With regard to the arrangement of information management (section 4), the key applicable matters are specifying the responsibilities relating to the system environment in requirement card TJ-02 (Security responsibilities), arranging up-to-date instructions in requirement card HT-04 (Security awareness) and supervision in requirement card TJ-07 (Compliance and data protection). On the other hand, requirement card TJ-03 (Security risk management) is directly applicable to the identification of risks associated with data processing and the risk assessment-based scaling of security measures.

Moreover, authority A has identified in its own risk management (section 13) that, for example, in order to achieve adequate fault tolerance and functional availability, it is possible to use requirement cards TJ-05 (Continuity management), KT-03 (Backup and recovery processes), MH-01 (Change management) and MH-02 (Systems development), as well as TT-02 (Protection against common network attacks). The monitoring of the state of information security (section 13) is directly supported by JT-01 (Traceability and detection capability). On the other hand, protection throughout the life cycle is materially linked to KT-04 (Vulnerability management) and SI-02 (Data destruction). On the one hand, A has identified that for reliable operation, access rights management requires user identification (IP-02). On the other hand, in order to reduce the attack surface of the system, network structure restrictions (TT-01) and systems hardening (JT-02) is unavoidable based on risks. Because the security of the system depends directly on the protections of the management connections (IP-03), A also considers these to be critical protections required of the system.

In its risk assessment (section 13), authority A has additionally identified that reliably ensuring the security of the information (section 15) also requires taking physical security (FT-01 – FT-05) into consideration, where applicable. In order for authority A to obtain certainty over the continuity and maintenance of security work, the security management subdivision can also be utilised, where applicable.

In its risk management, authority A has made a conscious choice that if the information system being developed would subsequently need to be transferred to another cloud service platform, this could cause significant costs and require significant rebuilding of the system. A accepts the risks associated with transferability and will not apply, e.g., requirement card SI-01 (Transferability) to this system.

Example 2: Assessment of the compliance of the protections of classified information

This section describes an example of how the criteria can be applied to the assessment of the compliance of the protections of classified information to be kept secret in terms of the requirements of the Act on Information Management in Public Administration (906/2019) and Government Decree on Security Classification of Documents in Central Government (1101/2019). The customer in the example is authority B which wants to assess the adequacy of the protections of its new information system for processing classified level IV (KÄYTTÖ RAJOITETTU) information to be kept secret. The new system is still in the design phase and is to be located on a cloud computing service.

Authority B has identified corresponding connections between the Act on Information Management (906/2019) in Public Administration and requirements compiled in PiTuKRi as authority A as described in example 1. Furthermore, authority B has identified the following direct connections concerning B's systems environment between the Government Decree on Security Classification of Documents in Central Government (1101/2019) and requirements compiled in PiTuKri:

- section 6: Preconditions for granting access to a classified document: EE-01 (System description); EE-02 (Legislation-derived risks)
- section 8: Handling rights and lists thereof: HT-05 (Need-to-know and separation of duties) / subsections 1–3; HT-04 (Security awareness); HT-03 (Non-disclosure agreements and secrecy commitments)
- section 9: Security areas: FT-01 (Defence-in-depth and risk management) / subsection 2; FT-03 (Prevention of unauthorised access)
- section 10: Protecting the handling of documents and information systems with security areas: FT-01 (Defence-in-depth and risk management), FT-02 (Structures and security systems), FT-03 (Prevention of unauthorised access), FT-04 (Service providers and visitors), FT-05 (Preparedness and continuity management); IP-03 (Management connections); JT-05 (Transfer and removal of protected information)
- section 11: Requirements concerning information systems and telecommunications arrangements / subsection 1: TT-01 (Structure of the communications network) / subsections 1 and 3
- section 11: Requirements concerning information systems and telecommunications arrangements / subsection 3: IP-01 (Access rights management) / subsection b.
- section 11: Requirements concerning information systems and telecommunications arrangements / subsection 5: IP-02 (User identification)
- section 11: Requirements concerning information systems and telecommunications arrangements / subsection 6: JT-02 (Systems hardening)
- section 11: Requirements concerning information systems and telecommunications arrangements / subsection 7: SA-01 (Encryption procedures and key management)
- section 12: Transfer of a data in a data network: SA-02 (Encryption outside a physically protected security area); SA-03 (Encryption within a physically protected security area); SA-01 (Encryption procedures and key management)
- section 15: Destruction of a document: SI-02 (Data destruction)

In addition, in protecting against electronic messages, such as e-mail attachment malware and also more direct attacks against the application security of the cloud computing service (1101/2019 / section 11 / subsection 2), key protections include TT-01 (Structure of the communications network), TT-02 (Protection against common network attacks), KT-04 (Vulnerability management), JT-04 (Protection against malware), JT-02 (Systems hardening), MH-02 (Systems development), and naturally also JT-01 (Traceability and detection capability).

On the other hand, in terms of protecting the integrity of the information system (1101/2019 / section 11 / subsection 4), the key method is physical security, to which sections FT-01 (Defence-in-depth and risk management), FT-02 (Structures and security systems), FT-03 (Prevention of unauthorised access), FT-04 (Service providers and visitors) and FT-05 (Preparedness and continuity management) are directly applicable. Outside physical protection, in addition to encryption (SA-02), e.g., IP-03 (Management connections) and JT-05 (Transfer and removal of protected information) must be taken into account in integrity protections.

Authority B has also clearly detected that the implementation of defence-in-depth (1101/2019 / section 7) requires mutually supporting protections for security management, both physical and information security, such as defence-in-depth and supervision of the data traffic network (TT-01: Structure of the communications network / subsections 2–3).

Annex 3: Assessment and accreditation by the competent authority

Background

Pursuant to the Act on the Assessment of the Information Security of Public Authorities' Information Systems and Telecommunications Arrangements (1406/2011),[36] the authorities may use only the Finnish Transport and Communications Agency Traficom, or an Information Security Inspection Body accredited by Traficom, for the assessment of its information system security. PiTuKri can be used as a tool when assessing how a cloud computing-based information system used or planned for the use of the authorities fulfils the national or international security requirements[37].

This Annex describes different PiTuKri use cases in the assessment of cloud computing-based information systems. The description focuses on the use cases of facility security clearance and assessment of public authorities' information systems, with Traficom as the competent authority. The description covers the assessment and accreditation processes as well as the accreditation by a competent authority. The description does not address other use cases, such as use as part of the organisation's internal security work.

Assessment process

Assessment process for the security of information systems (L 1406/2011) begins when the target of the assessment submits an assessment request to Traficom. Other main phases of the assessment process are planning of assessment, the inspections and reporting. The assessment process is visualised in a simplified form in Figure 4. The assessment process may be used for purposes such as supporting the internal security work of the target organisation, with the addressing of residual risks completely within the responsibility of the target organisation. The assessment process is described in more detail in the guideline on the NCSA's information security assessments from the customer organisation's perspective (in Finnish only)[38].

Figure 4. Simplified assessment process.

[36] Act on Information Security Inspection Bodies (L 1405/2011), https://www.finlex.fi/fi/laki/ajantasa/2011/20111405.

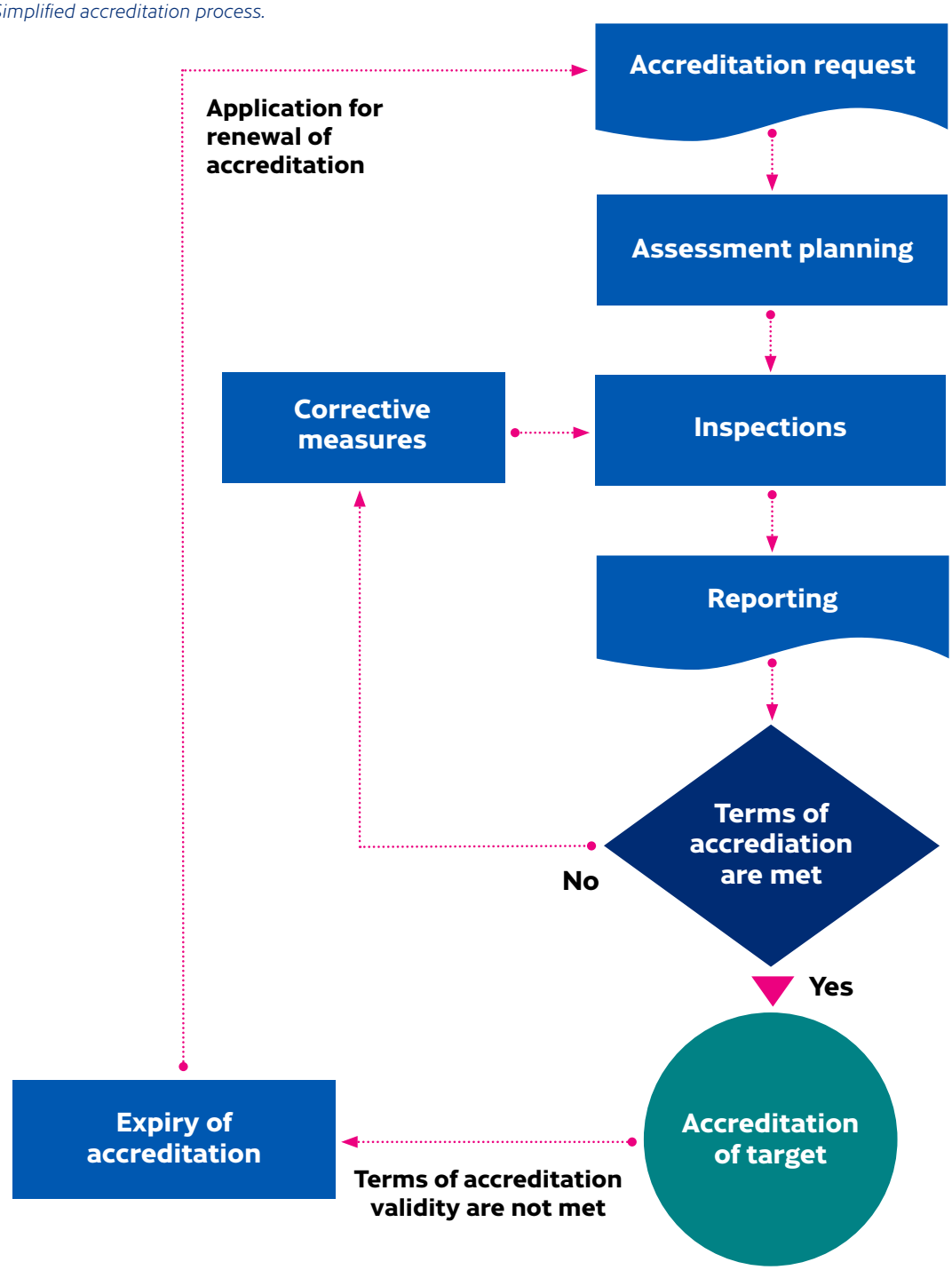
[37] Act on International Security Obligations (588/2004), https://www.finlex.fi/fi/laki/alkup/2004/20040588. Security Clearance Act (726/2014), https://www.finlex.fi/fi/laki/alkup/2014/20140726.

[38] National Cyber Security Centre. 2019. URL: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/ohje_NCSA-toiminnon_suorittamat_tietoturvallisuustarkastukset.pdf.

Accreditation process

An accreditation process aiming for accreditation by the Finnish Transport and Communications Agency Traficom (Act 588/2004 or 1406/2011) begins when the target organisation submits an accreditation request to Traficom. The accreditation process is similar to the assessment process except that any deviations observed in the inspections must be corrected and the corrections verified before the accreditation can be issued. The accreditation process is shown in a simplified form in Figure 5. The accreditation process may be utilised, for instance, when the target organisations wants to demonstrate the adequacy of its protections by an accreditation issued by Traficom. In the accreditation process, risk assessment is carried out using the assessments by the target organisation and Traficom alike. The accreditation process is described in more detail in the guideline on the NCSA's information security assessments from the customer organisation's perspective (in Finnish only).

Figure 5. Simplified accreditation process.



Accrediation by a competent authority

The Finnish Transport and Communications Agency Traficom may issue an accreditation to a system that processes national or international classified information and meets the requirements. An accreditation may be issued only in the event that the target of the assessment undertakes to maintain the approved security level. Typically[39], it is also required that the entire system is governed under Finnish legislation.

The validity of the accreditation expires if any significant changes that affect the security of the inspected target occur. Major changes to the network structure, personnel, security procedures or premises are examples of such changes. Changes caused by normal maintenance, such as installations of software security patches, do not lead to expiry of a valid accreditation. Case-specific terms for the expiry of accreditation are specified in connection with issuing the accreditation. Approvals for any significant changes must be requested in advance from Traficom.

[39] An example of an exception to this are system projects associated with international cooperation between authorities, in which the jurisdiction and responsibility concerning the assessment and accreditation of the system parts has been separately agreed between the security authorities of the Member States taking part in said cooperation between authorities.

Finnish Transport and Communications Agency Traficom

National Cyber Security Centre

PO Box 320, FI-00059 TRAFICOM
p. +358 29 534 5000
traficom.fi

TRAFICOM
Finnish Transport and Communications Agency
National Cyber Security Centre